Network and Protocol Reference

Network General Corporation

Network and Protocol Reference

Network and Protocol Reference

July 1996

Part Number: 3005303

Table of Contents

Chapter 2. Major Protocol Suites

List of Figures

Chapter 1. Network Architectures

Chapter 2. Major Protocol Suites

List of Tables

Preface

Chapter 1. Network Architectures

Preface

About This Manual

Network General's *Network and Protocol Reference* provides background information on a broad spectrum of network types and communication protocols. You will want to refer to it from time to time to help you get the most out of your Sniffer® Network Analyzer or Distributed Sniffer System®.

This manual is intended as a reference volume; you most likely will not use it on a daily basis. For information on how to operate your Sniffer Network Analyzer or Distributed Sniffer System, turn to the operations documentation provided with your product shipment.

Organization of This Manual

Table i describes the organization of this manual.

Table i. Scope of Each Chapter or Appendix in this Manual

Chapter/Appendix	Contents
Chapter 1, "Network Architectures"	Covers basic knowledge about local and wide area network architectures.
Chapter 2, "Major Protocol Suites"	Covers basic knowledge about network protocols and protocol interpreters.
Appendix A, "Glossary of Terms"	Provides a glossary of data communications terminology.
Appendix B, "Bibliography"	Provides a bibliography of source material.

Other Sources of Information

Network General provides other sources of information to help you become familiar with the Sniffer Network Analyzer.

Technical Support

Network General® Corporation's Technical Support personnel are available from 6 a.m. to 6 p.m. Pacific time, weekdays. Technical Support is available via telephone, FAX, FAX-on-Demand, TDD for the hearing impaired, Internet mail, electronic bulletin board, and the World Wide Web home page. Outside of support hours, you may leave a voice message. Our Technical Assistance Centers are located in California and the United Kingdom.

If you purchased your Network General® Corporation product from one of our International Distributors, you must contact that distributor for support assistance. Please review our World Wide Web site at http://www.ngc.com for information on contacting our International Distributors. Table ii. describes the various ways to access Technical Support.

Table ii. Network General Technical Support Department

North American and International, 0600–1800 (PST), Monday–Friday

Telephone Number (North America only)	+1-800-395-3151
Telephone Number (other International)	+1-415-473-2090
FAX	+1-415-327-9436
FAX-on-Demand (North America)	+1-800-764-3329
FAX-on-Demand (other International)	+1-415-473-2690

Europe, 0530–1730 (GMT), Monday–Friday

Telephone - France (toll-free)	+33-05-90-27-91
Telephone - Germany (toll-free)	+49-01-30-81-92-37
Telephone - Switzerland (toll-free)	+41-1-55-00-29
Telephone - other Europe	+44-17-53-86-36-01
FAX	+44-17-53-86-34-07
FAX-on-Demand	+1-415-473-26-90

Worldwide

TDD for the hearing impaired	415-327-8723
SniffNet BBS (300 to 14,400 bps)	415-327-3875
Internet Address	support@ngc.com
World Wide Web (Internet) information	http://www.ngc.com

World Wide Web

You can obtain additional information about Network General and its products and services from the World Wide Web at *http://www.ngc.com.*

Training

Network General offers a comprehensive set of training courses focused on hands-on network analysis, monitoring, and troubleshooting using the Foundation family of products and Distributed Sniffer System. Courses can be conducted at your site, at central locations throughout the globe, or at training centers in Menlo Park and Anaheim, California; Chicago, Illinois; and Atlanta, Georgia. For more information about these courses, contact your sales representative or call Network General Corporation.

Chapter 1
Network Architectures

Overview

The network reference material in this chapter covers the physical and data link layers of various network types. Each section summarizes the features of each particular network and the variations related to its use and understanding.

Ethernet Network Architecture

Ethernet is a type of local area network (LAN) suitable for high-speed interconnection of computers and computer-controlled devices over moderate distances. The Ethernet architecture is defined by implementations from many manufacturers as ANSI/IEEE standard 802.3, ISO/DIS standard 8802/3, and FIPS standard 107.

There are several variations permitted by the standards and other variations that are not official but are, nonetheless, popular. To say that a network is an "Ethernet" means only that it is one of several closely related, but not necessarily compatible, LANs. Even use of the word "Ethernet" may be confusing, since it is sometimes reserved to refer to the earlier DEC/Intel/Xerox (DIX) network, leaving 802.3 networks to designate the others.

Some system implementations of the Ethernet network also use at least a subset of a similarly standardized protocol for Logical Link Control (LLC) as defined by ANSI/IEEE standard 802.2 and ISO/DIS standard 8802/2.

Physical Interconnection and Speed

Stations connected to a conventional Ethernet network are all connected to the same bus, so that every station "hears" what any station transmits. The delay between transmission and reception depends only on the propagation delays through the wires and attaching devices. It differs fundamentally, however,

from networks like the IEEE 802.5 token ring, where stations are wired in a *logical ring* so that each station only hears what its upstream neighbor transmits (see "Token Ring Network Architecture" on page 1–10).

The most common Ethernet transmission speed is 10 megabits per second (Mbps), or 1,250,000 bytes per second, sent in baseband (non-modulated, non-RF) form.[1] The ANSI/IEEE documents refer to this as the *10BASE5* (10 Mbps, baseband, and 500 meters per segment) standard. A second standard is 10BASE2 (10 Mbps, baseband, and 185 meters per segment). A third standard is *10BASE-T* (10 Mbps, baseband, over twisted pair). Network General's Ethernet Sniffer analysis application supports 10BASE5 networks, 10BASE2 networks, 10BASE-T networks, and some variants of them. The 100BASE-Tx network provides up to 100 Mbps.

Thick Ethernet

There are two common schemes for the wiring of stations into an Ethernet. The original *thick Ethernet* scheme uses a backbone of yellow, semi-rigid, 0.4-inch diameter coaxial cable segments for up to 100 stations per segment. Each segment can be a maximum of 500 meters long, and segments may be connected with repeaters, subject to the restriction that there are no more than two repeaters in the path between any two stations. Thus, the maximum total cable length between two stations is 1500 meters but is often less than that in practice because of the way the cable is routed. The cable impedance is 50 ohms, and segments must be terminated on each end with a 50-ohm terminator attached with an N-series coaxial connector. The shield conductor must be grounded to an earth reference at only one point and fully insulated everywhere, including at connectors and terminators, to prevent shock hazards.

A station is connected to a thick Ethernet cable by means of a *transceiver*, which is a signal converter that must be attached directly to the cable. Transceivers are called *medium attachment units* (MAUs) by the IEEE Standards documents. Many transceivers clamp on to the cable and use a *vampire tap* to make contact with the outer shield and inner conductor without requiring that the cable be cut. The spacing between transceivers must be a multiple of 2.5 meters; the yellow cable has black marks to indicate possible transceiver attachment points.

A single station is connected to its transceiver with a more flexible 4-pair *drop cable* or *Attachment Unit Interface* (AUI) *cable* whose maximum length is 50 meters. In addition to carrying network data in each direction on separate

1. Because of the access control mechanism, the effective network throughput is significantly less than the transmission speed.

pairs, the drop cable also supplies power for the transceiver electronics from the equipment being attached to the network. Both ends of the drop cable use DB-15 connectors: a male connector with locking posts for the equipment end and a female connector with a slide latch for the transceiver end. Note that the slide latch is often too big for the back panel of personal computers, so at least two variations of this attachment scheme are in common use.

To reduce the per-station cost of the transceiver and to circumvent the limit of 100 stations per segment, transceiver fan-out boxes are available. These typically allow four or eight drop cables to be connected to a single box that is connected to a standard transceiver clamped to the coaxial cable segment.

Thin Ethernet

Another approach to reducing the cost of an Ethernet installation is *thin Ethernet*, "cheapernet," or 10BASE2. It dispenses with the large, semi-rigid coaxial cable and separate external transceivers. Instead, it uses flexible RG-58/U coaxial cable and transceiver circuitry built into each attaching computer. For this wiring scheme, the overall topology is still a linear segment but the segment passes by the back of each computer. Attachment is made by splicing BNC connectors into the cable and inserting a "T" connector. The segments are still terminated with 50-ohm terminators at each end. The maximum length of a segment is usually 185 meters, although some vendors support longer distances.

Cheapernet transceivers are generally part of the network adapter circuitry, and the exposed connector is a female BNC. A hybrid approach is also possible, since there are *thin Ethernet transceivers* available that attach with a standard drop cable to an attaching computer but have a female BNC instead of a *vampire tap* for connecting to the network. There are also *thin to thick adapters* that allow segments to be built out of both kinds of cable. Some devices provide both a BNC connector (for thin Ethernet) and a DB-15 (AUI) connector (for a thin- or thick-Ethernet transceiver). On most Ethernet adapter cards supplied by Network General, you determine which connector is active by the position of a jumper. See the Installation Guide accompanying your product shipment for exact information.

Twisted Pair Ethernets

Ethernet over twisted pair has been standardized by an IEEE 802.3 project, known as the 10BASE-T standard. The standard provides a means for attaching AUI-compatible devices to 24 gauge, unshielded twisted-pair cable, instead of the usual coaxial media.

Stations connect their standard AUI connector to a special twisted-pair transceiver (called a *Twisted Pair MAU* by the IEEE Standard documents) that

has an RJ-45 phone jack for the other connection. The transceiver is then wired to one port of a *multiport repeater* (MPR) typically located in a wiring closet. The MPRs can in turn be wired to higher-level MPRs. The resulting network topology is a distributed star, where each twisted-pair cable is allowed to be up to 100 meters long. Note that this is physically unlike the original multidrop Ethernet but can be centrally managed more easily and has higher reliability.

There are other twisted-pair Ethernet architectures that predate those previously mentioned; LattisNet from SynOptics Communications is one example. Most computers (and network analyzers) with an AUI interface can be used interchangeably on any of these networks with the appropriate transceiver.

Other Ethernets

Ethernet variations proliferate both with and without benefit of official standardization. Most share at least a philosophical tradition with the Ethernets discussed above but are often incompatible in the sense that equipment designed for one species cannot be connected with equipment designed for another. Among these are:

- Broadband Ethernets, some of which run at 5 Mbps so as to fit within a single television channel assignment.
- Fiber-optic Ethernets, most of which use two cables per station and a centralized optical coupler to rebroadcast the transmitted signal to all receivers.

Access Control

Ethernet and its variants use an algorithm to control transmission called *carrier sense multiple access with collision detection* (CSMA/CD). A similar architecture is *carrier sense multiple access with collision avoidance* (CSMA/CA). Apple Computer implemented CSMA/CA in its LocalTalk® network using the LocalTalk Link Access Protocol or LLAP.

Before transmitting, a station waits until it hears no other station transmitting. It defers until it senses no carrier from another station and then sends its message. Since there is the possibility that another station may decide to transmit at roughly the same time, the sending station monitors the network to hear if its own message appears on the network ungarbled. If it detects a collision with another message, it intentionally sends a few additional bytes (a process called *jamming*) to ensure propagation of the collision throughout the system to all other transmitting stations. The station then remains silent for a

randomly determined amount of time (controlled by a *backoff algorithm*) before attempting to transmit again.

Collisions may be heard by receiving stations as badly-formatted frame fragments called *runts* that are typically shorter than the minimum frame size and have incorrect check sums. These frames may also have an incorrect starting sequence and may not be seen as the start of a frame at all. Note that the propagation time through an Ethernet network is typically much longer than the transmission time for a bit. Therefore, different receivers will see different effects depending on their position relative to the various transmitters.

In addition to deferring to active traffic, stations wait before beginning transmission after the end of another transmission. The pause varies according to network type: for example, 9.6 microseconds for Ethernet. This enforced interframe spacing allows time for receivers to recover from one frame and to prepare to receive the next.

Other Transceiver Functions

Besides moving serial data to and from the attached device and the network, the transceiver (or MAU) has several other functions:

- ***Collision detection:*** One wire pair in the drop cable transmits the *collision detect signal* (called *signal quality error*, SQE, in IEEE documents) from the transceiver to the device. In addition to its use to control transmission, this signal can also be used to detect some network and transceiver failures. A transceiver that supports the *signal quality error test* feature will generate a collision detect signal at the end of a transmitted frame to demonstrate that the collision detect circuitry is at least partially operational.
- ***Jabber detection:*** The transceiver is required to disable transmission if the device transmits for longer than the longest possible frame. This prevents some kinds of device failures from halting network activity but is not foolproof.

Format of a Frame

All data in a frame is transmitted as a sequence of 8-bit bytes starting with the least significant bit. The format of each frame is shown in Figure 1–1.

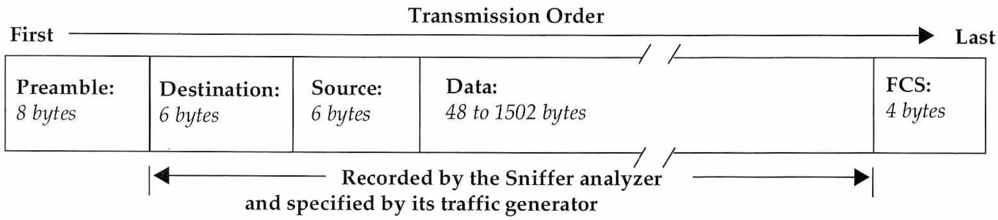


Figure 1–1. Frame Format for Ethernet

The **preamble** is a fixed data pattern used for receiver synchronization and recognition of the start of a frame. The **destination** and **source** addresses are each 6 bytes. Various kinds of multicast addresses are indicated if the first transmitted bit (the low-order bit of the first byte) of the destination address is a one. Note that the IEEE 802.3 standard also permits 2-byte source and destination addresses, but their use is rare and inconsistent with 10BASE5 and 1BASE5.

If the first transmitted bit of the source address is a one, it indicates that a *routing information* (RI) field is present before the data field. This is a convention inherited from token ring. Such frames are generally seen on an Ethernet only when forwarded over a MAC-level bridge from a token ring.

The **data** field must have a minimum number of bytes so that the duration of a frame is longer than the worst-case propagation delay (45 microseconds for Ethernet) through the network. For Ethernet the minimum must be 48 bytes so that the frame is at least 60 bytes (excluding the **preamble** and the **FCS**). If this were not true, then collisions might not be detected. The IEEE 802.3 standard specifies other limits on the frame size for non-10BASE5 and non-1BASE5 networks only.

Following the data is a 4-byte *frame check sequence* (**FCS**) that checks the validity of the source, destination, and data fields. Network General's Sniffer analysis application does not record the **FCS** but will optionally collect and identify frames whose **FCS** is incorrect.

Format of the Data

To specify how the initial bytes of the data field are to be interpreted, there are several conventions in general use. The original format as defined by Xerox, now often called the "Ethernet" format (in contrast to the IEEE 802.3 format),

contains no length field and begins with a 2-byte **Ethertype** field that indicates the major protocol type (Figure 1–2). For example, the IP protocol of TCP/IP is assigned the Ethertype hex 0800.

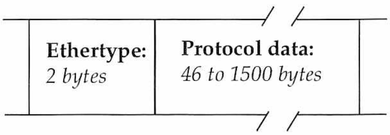


Figure 1–2. Original "Ethernet" Data Format Defined by Xerox

The assignment of Ethertypes to protocols was originally done by Xerox and has now been taken over by the US Defense Communications Agency.

The second convention for interpretation of the data field is that supported by the IEEE/ANSI/ISO standards organizations for 802.3 networks and begins with a 2-byte **length** field (most significant byte first), followed by a *Logical Link Control* (LLC) header that conforms to the IEEE 802.2 standard (Figure 1–3).

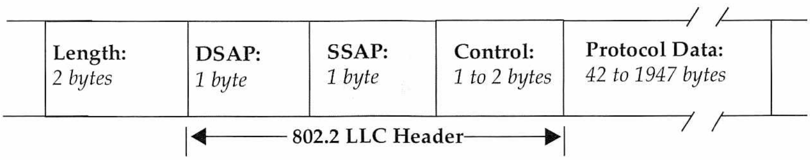


Figure 1–3. IEEE 802.3 Data Format Defined by IEEE/ANSI/ISO Standards Organizations

Although both data formats can and do appear on the same network, there is no foolproof way to distinguish between the two by looking at the frame. In practice, though, almost all assigned Ethertypes are numerically larger than the maximum frame length of 1500. Thus, if the first two bytes of frame data are larger than 1500, it is probably an Ethernet/Ethertype frame. (The only common exception is the PUP Ethertype, hex `0200`.)

Network General's Sniffer analysis application decodes frames in either format and makes the format decision automatically unless instructed otherwise by the operator.

For frames of either type, the embedded **protocol data** represents information that is interpreted by higher level protocols and may contain many other such nested levels.

LLC Frames

A frame that conforms to the 802.2 standard is an LLC frame. LLC is a protocol that provides reliable connection-oriented virtual circuits or connectionless datagrams between processes. It is a subset of the International Standards Organization-defined superset, *High-level Data Link Control* (HDLC). See the subsection on HDLC and two other HDLC subsets, SDLC and LAPB, in, "WAN/Synchronous Architecture" on page 1–20.

The **protocol data** part of LLC frames (see Figure 1–3) begins with a 3- or 4-byte header, the first two bytes of which are the *destination service access point* (**DSAP**) and *source service access point* (**SSAP**). The SAP numbers are preassigned codes that indicate which subprotocol is used in the rest of the frame. For example, the NetBIOS protocol has been allocated a single SAP (hex F0), and Systems Network Architecture (SNA) has been allocated four SAPs (hex 04, 05, 08, and 0C). The **SSAP** often equals the **DSAP**, except in frames that are establishing an initial SNA connection.

The **control** field defines the exact function of LLC frames. The three LLC frame types are described below.

Information

I format frames are used to send arbitrary sequenced data interpreted by the protocol that the SAPs designate. The LLC header contains a *send* sequence number N(S) for this frame and a *receive* sequence number N(R) of the next frame expected from the other station.

Supervisory

S format frames contain or consume an N(S) number but do contain an N(R) number. In addition, they can contain the indications shown in Table 1–1 as either a command or a response:

Table 1–1. Indications Used in LLC Supervisory Frames

Command/Response	Action
RR	*Receive Ready.* Transmission of Information frames can proceed.
RNR	*Receive Not Ready.* Transmission is temporarily blocked.
REJ	*Reject.* Retransmission starting with N(R) number is requested.

Unnumbered

U format frames contain neither N(S) nor N(R) numbers but may contain control information or data. The commands and responses in the unnumbered frame format are shown in Table 1–2.

Table 1–2. Commands and Responses in LLC Unnumbered Frames

Command/Response	Action
SABME	*Set Asynchronous Balanced Mode (Extended).* Establish a virtual connection, also called a link.
DISC	Disconnect. Terminate a virtual connection.
DM	*Disconnected Mode.* The connection is broken.
UA	*Unnumbered Acknowledgment.* For SABME and DISC response.
FRMR	*FrameReject.* The format of a received frame was invalid. The protocol data field contains the reason.
XID	*Exchange Identification.* Used between two stations to exchange identification and the characteristics of the two stations.
TEST	*Test Probe.* Should be echoed by the receiving station.
UI	*Unnumbered Information.* Used by the SAP protocol for any purpose.

The only LLC frames that are allowed to contain data after the LLC header are I, UI, TEST, XID, and FRMR types.

There are three types of LLC operation. The first is known as *unacknowledged connectionless service*. This is the minimal use of LLC in which every frame is a UI type. Thus, the data part of every frame viewed with the Sniffer analysis application begins with three bytes: the two SAP bytes and a UI (hex 03) control byte. This technique is typically used to implement higher level protocols that do connection control and sequencing themselves, and therefore do not need the services of the standard LLC, but that prefer compatibility with LLC formats.

The other two types carry more overhead. *Connection-oriented service* provides flow control, sequencing, and error recovery. *Acknowledged connectionless service* is also connectionless like the first type but provides for acknowledgment and relieves higher layers of that responsibility.

Assignment of Network Addresses

The modern convention for 6-byte node addresses is to divide them into an initial 3-byte code representing the manufacturer of the equipment, and a unique 3-byte serial or sequence number assigned to that piece of equipment. The responsibility to assign manufacturer codes was initially taken by Xerox but has now been assumed by the IEEE.

It is the intention of the IEEE that the same code be used for all networks supported by a manufacturer, including Ethernet (IEEE 802.3) and token ring (IEEE 802.5). However, Ethernet bytes are transmitted with the least significant bit first, and token ring bytes are transmitted with the most significant bit first. This has led to considerable confusion in the way that assigned addresses are used.

The IEEE's stated position is that the assigned code specifies how the address should appear on the network cable. The result is that a network address stored in a computer's memory will be different, depending on what the originating network was. Since network addresses appear at various places within the protocol levels of a frame, and since a frame may have been forwarded by various network types, this imposes a difficult burden on network software. In fact, observation of network software and hardware from a variety of vendors shows that some have chosen to use the same address as it appears in memory on both networks, thus using a code on one or the other network that, according to the IEEE interpretation, is not assigned to them.

Token Ring Network Architecture

The token ring is a type of LAN suitable for high-speed interconnection of computers and computer-controlled devices over moderate distances. The token ring architecture is defined by implementations from IBM, Texas Instruments, and others as ANSI/IEEE standard 802.5 and ISO/DIS standard 8802/5.

Most system implementations of the token ring network also use at least a subset of a similarly standardized protocol for LLC and defined as ANSI/IEEE standard 802.2 and ISO/DIS standard 8802/2.

Physical Interconnection and Speed

Stations connected to the token ring network are wired together physically in star-like fashion. Each station uses one cable to attach itself to a nearby *passive concentrator*, or *multiple access unit* (MAU).[1] The MAUs can be linked together and may be separated by moderate distances. The number of stations and the distance limitations depend on several variables, including cable type, but typically one or two hundred stations can be interconnected into a single network segment using cables between stations and MAUs up to 300 meters long. The distance limitations can be overcome by using special line drivers or fiber-optic cables. Networks of many hundreds or thousands of stations over long distances can be created using bridges between network segments.

One type of connector used to attach to MAUs was the IBM Data Connector, designed by IBM. These connectors are hermaphroditic, so that any two may be joined; cable "extension cords" have the same connector on both ends. The cable that connects to a particular computer may use the hermaphroditic connector if there is enough panel space for the mating connector (about one inch by one inch) or may use a non-standard connector. The convention for personal computers is to use a DB-9 female connector on the backpanel and DB-9 male on a cable whose other end has the hermaphroditic connector. Other vendors have built MAUs with RJ-11 connectors that use less panel space.

There are two basic speeds for the network: 4 Mbps, or 500,000 bytes per second, and 16 Mbps, or 2,000,000 bytes per second. This does not include the many levels of overhead in a typical application, and throughput for the user will often be many times less than that. There is nothing in the hardware or software architecture that limits the network to 16 Mbps.

Stations operating at 4 and 16 Mbps may not be attached to the same token ring at the same time. The first station to become operational on the ring establishes the speed, and any subsequent station entering the ring at a different speed will cause transmission errors and will often result in other stations removing themselves from the ring. Unfortunately, current ring adapters have no provision for determining the speed of an established ring before attempting to join it.

1. Do not confuse this use of the MAU acronym with Medium Attachment Unit (MAU) defined in IEEE Standards documents for Ethernet.

Logical Interconnection

Each interconnection cable contains two twisted pairs of wires. Although the stations and MAUs are cabled in a star-like fashion, the electrical effect of the token ring cables and connectors is to create a continuous ring from station to station. One twisted pair in the cable to each station is used to transmit to the next station in the ring, and the other pair is used to receive from the previous station. The ordering depends on how cables are plugged into the MAUs and how the MAUs are interconnected.

The operation of the ring depends on each station retransmitting data from its *receive pair* onto its *transmit pair*, regardless of whether that station is involved in the conversation. To insure that the ring is operational even when some stations are turned off, connecting a cable from a station to a MAU is not sufficient to cause that station to enter the ring; it also must send a DC voltage on its transmit pair to trigger a relay in the MAU. If power to the station fails, or if the cable to the station is disconnected at either end, the relay loses power and the ring bypasses that station.

When the relay is not powered, the cable to the station has its transmit pair connected to its own receive pair so that it may test the network adapter and cable. Prior to inserting itself onto the ring by supplying the relay voltage, the network adapter sends several thousand data frames to itself to verify correct operation. This process, plus the network adapter self-test, may take 15 seconds or more.

Access Control

Only one station on the entire ring is allowed to transmit data at a time. To control access, a 3-byte message giving permission to transmit, called the *free token*, continually circulates when there is no other traffic. Each idle station retransmits it as it is received. A station that wants to transmit data waits for the token and then sends its data instead of the token. When its data transmission is finished, it regenerates the token message. In addition to this simple rotational priority scheme, there are also ways to establish other priorities. Every message (including the token) contains both a 3-bit priority field for itself and a 3-bit reservation priority for a possible subsequent message.

A data message, called a *frame*, may be directed to a single destination station or to any of various groups of stations. In all cases, the addressee (the station that receives the message) does *not* remove it from the ring. It simply makes a local copy of the message and retransmits it. The originating station is responsible for removing the message from the ring when the message returns to it. The originator then replaces the message with the token.

In visualizing the traffic flow on the network, it is important to realize that most frames are much longer (in time) than the round-trip delay around the ring, particularly at 4 Mbps. Each station introduces a delay of less than 3 bit times when it is repeating data from its receive cable to its transmit cable, whether or not it is making a copy of the data. That delay for each station, plus the cable propagation delays, produce the total ring round-trip time. For a typical network of 50 stations, the round-trip time might be about 50 microseconds. A 1000-byte (8000 bit) frame takes 2000 microseconds to transmit at 4 Mbps, so the transmitter must be removing the beginning of the frame that has made the trip around the ring long before it has finished sending out the whole frame.

At 16 Mbps, small frames will take less time to transmit than the round-trip token timing, especially for large networks. To improve performance, the newer token ring adapters implement an *early token release algorithm* that allows them to transmit the free token to the next station before they have received a frame just transmitted.

In normal operation, the token is circulated and regenerated by the cooperative operation of all stations acting democratically. If the token is destroyed by transmission error or other fault (a station attaching or removing from the ring typically destroys the token because of electrical noise created by the relay operation) it is the responsibility of a station designated as the *active monitor* to notice the absence of the token and to regenerate it. There is only one active monitor on the network at a time, although every station is able to assume the role if needed.[1] If the active monitor is disabled or leaves the ring, a monitor contention process begins through which a new active monitor is elected by the remaining stations.

Format of a Token Frame

All data is transmitted as a sequence of 8-bit bytes sent serially and Manchester encoded. The minimum transmission is the 3-byte *token* (Figure 1–4).

SDEL *1 byte*	**AC** *1 byte*	**EDEL** *1 byte*

Figure 1–4. Frame Format for a Token Frame

Both *starting delimiter* (**SDEL**) and *ending delimiter* (**EDEL**) have intentional Manchester code violations in certain bit positions so that the start and end of

1. The Sniffer analysis application cannot play the role of active monitor when in capture mode.

a frame can never be accidentally recognized in the middle of other data. The *access control* (**AC**) byte contains a bit that indicates that this is a token, not a data frame, and contains priority information. Tokens are not recorded by the Sniffer analysis application.

Format of a Data Frame

If a message is not a token, then it is a *data frame* (Figure 1–5).

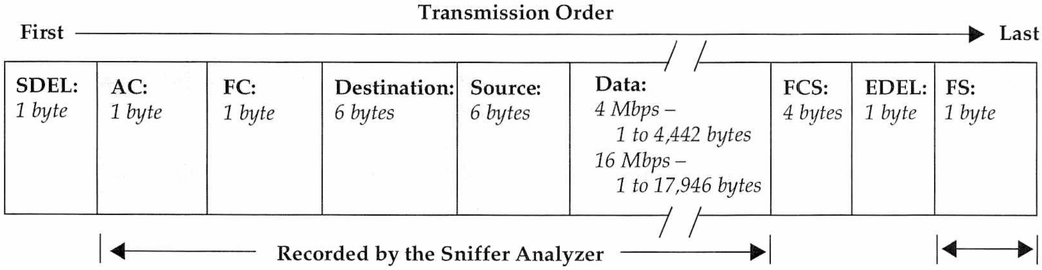


Figure 1–5. Frame Format for a Token Ring Data Frame

The **SDEL**, **AC**, and **EDEL** fields are as before, except the **AC** byte now says that this is a data frame and not a token. The **FC** byte contains frame information. The **destination** and **source** addresses are each 6 bytes, and various kinds of *multicast* or *broadcast* addresses are indicated if the first bit of the destination address is a one. Following the **data** field is a *frame check sequence* (**FCS**) that checks the validity of all previous data starting with the **AC** byte. The Sniffer analysis application records bytes starting with **AC** and ending with the last byte of the data field.

The last byte for data frames is the *frame status* (**FS**) byte containing bits that may be set *on* by the recipient of the frame: *address recognized,* if a station matched the destination address and *frame copied* if it was able to successfully make a local copy of the data as it passed by. Note that the **FS** is not covered by the frame check sequence (so that the **FCS** does not have to be changed by the recipient), but for greater reliability, the bits in the **FS** are each duplicated. The Sniffer analysis application records the **FS** byte and displays it in the **detail** view.

Optional Routing Information

Token ring uses a technique known as *source routing* when it does routing. Thus, there is an optional *routing information* (**RI**) field that may be present at the beginning of the data part of any frame. The **RI** field, which may be up to 32 bytes long, contains information about the path that the frame took if it was

forwarded through multiple network segments by bridges. If the **RI** field is present, the first bit of the source address will be a one.

The **RI** field is not part of the IEEE 802.5 token ring standard, although it has been proposed for official adoption. IBM software currently uses this extension to the standard.

MAC Frames

A data frame may be a *medium access control* (MAC) frame that contains information used to control the token ring network itself. Most MAC frames are generated and processed by the computer's network adapter and are not of concern to software within the host. The type field in the FC byte indicates whether the frame is a MAC frame.

MAC frames are used for processes like *monitor contention*, *error reporting*, and *error recovery*. In addition, the *active monitor* announces its presence with a periodic MAC frame, and all stations that could become the monitor (for example, *standby monitors*), should the need arise, do likewise.

MAC frames contain a major type code followed by a variable number of variable-length fields called *subvectors* that give additional information.

LLC Frames

A data frame that is not a MAC frame is (in all non-proprietary uses of the token ring network) an LLC frame. See the discussion of the LLC frame format in "Format of a Frame" on page 1–6. Since all non-MAC frames are supposed to use 802.2 LLC, an alternative mechanism has been standardized for encapsulating the older Ethertype formats. This mechanism is known as the Subnetwork Access Protocol (SNAP). The LLC frame format for SNAP is shown in Figure 1–6.

DSAP: *hex AA*	**SSAP:** *hex AA*	**Control:** *hex 03*	**Agency code:** *3 bytes*	**Local code:** *2 bytes*

			← **Protocol Identification Header** →	

Figure 1–6. LLC Frame Format for Subnetwork Access Protocol (SNAP)

SNAP has been assigned **SAP** hex AA, and the data field following the **Control** field is a 5-byte *protocol identification header*. The **Agency code** is an assigned manufacturer code, but sometimes 0 is used. The **Local code** is typically the Ethertype. Ethernet-style data follows the header.

Assignment of Network Addresses

For a discussion of the assignment of network addresses, see "Assignment of Network Addresses" on page 1–10.

Fiber Distributed Data Interface Network Architecture

Fiber Distributed Data Interface (FDDI) is a LAN standard suitable for high-speed interconnection of multivendor LANs over moderate to long distances. The FDDI architecture is defined by implementations of the ANSI/ISO X3T9 standards.

The FDDI standards define a version of the Physical and Data Link layers of the OSI model. The FDDI standards consist of the following:

- Physical Layer Medium Dependent (PMD) defines the medium requirements, the connectors that attach the nodes to the medium, and the fiber-optic transceivers.
- Physical Layer Protocol (PHY) defines the symbols, line states, data framing, clocking requirements, and encoding/decoding techniques.
- Media Access Control (MAC) defines the data link packets required for token passing, frame formatting and checking, data link addressing, error detection and recovery, and bandwidth allocation among nodes.
- Station Management (SMT) defines how to manage the PMD, PHY, and MAC portions of FDDI. SMT facilities include connection management, node configuration, error recovery, and formatting of SMT frames. SMT also includes a Management Information Base (MIB).

Figure 1–7 shows the relationship among the FDDI standards and how they combine to form the FDDI specification. Although Logical Link Control (LLC) is not part of the FDDI standards, FDDI requires LLC for proper operation and data transmission.

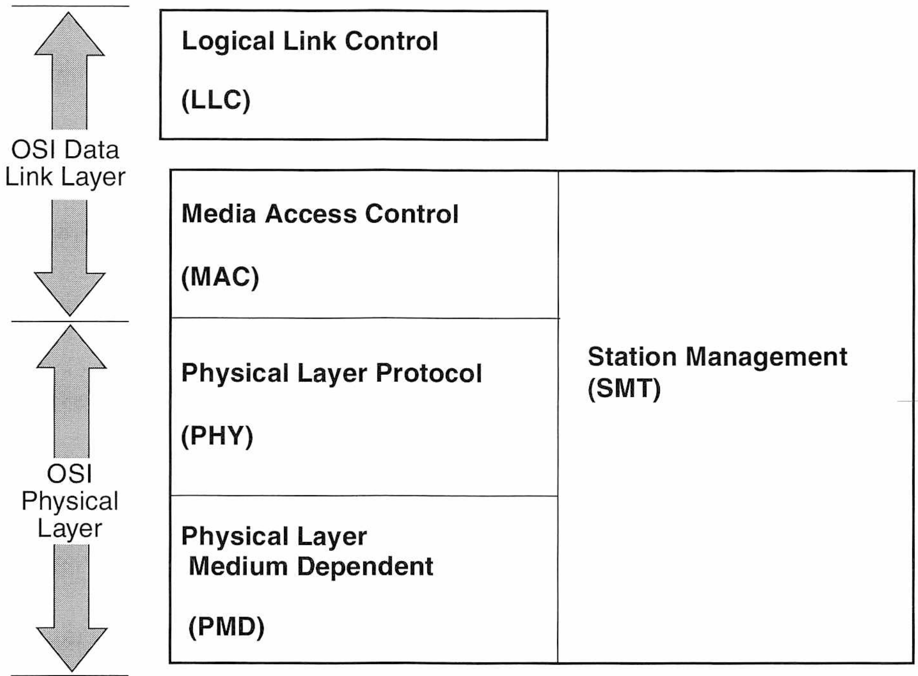


Figure 1–7. Relationship of FDDI Standards

Physical Interconnection and Speed

Physically, an FDDI network can have a ring, star, or tree topology. An FDDI network can consist of a concentrator with attached stations, a tree of concentrators, a dual counter-rotating ring, or a dual ring of trees. The dual counter-rotating ring provides a fault-tolerant structure that ensures data flow in case of a cable or station failure on the ring.

Stations attached to an FDDI network are physically connected by a media interface connector (MIC). A MIC aligns the fiber with the transmit/receive optics in the station. The connector consists of a keyed plug and a keyed receptacle.

Logically, stations are connected to Media Access Control (MAC) entities. Each MAC has a unique data link address. The MACs are interconnected in a token ring configuration— each MAC receives tokens and data from its upstream neighbor and transmits tokens and data to its downstream neighbor. A station can have multiple instances of PMD, PHY, and MAC entities, but only one instance of SMT.

FDDI operates at 100 MBps over a fiber-optic cable. The ANSI standard defines the fiber medium as 62.5/125 micrometer, multimode, graded-index, fiber-optic cable.

Access Control

The FDDI standard specifies a timed-token passing method for controlling access to the ring. Stations compete for the right to initialize the ring through a mechanism known as the claim process. During the claim process, each station continually transmits "claim frames" containing that station's required target token rotation time (TTRT). If a station receives a claim frame with a lower TTRT than its own, it stops transmitting its own claim frames and simply repeats the claim frames that it receives. When a station receives its own claim frame, it surmises that its value of TTRT is the lowest one and that, in accordance with the FDDI rules, it can therefore initialize the ring.

To initialize the ring, the station issues a token. The token passes around the ring without being captured by any station. After the token's third rotation, the ring is in a steady-state operation and stations can begin transmitting data.

In normal operation, the token is circulated and regenerated by all active stations on the ring. If a station wants to transmit data, it waits until it detects the token. It then captures the token and stops the token passing process. The station can then send data frames until it has finished sending data or until its token holding time (THT) expires. Then the station releases the token onto the ring for use by another station.

Format of a Token Frame

The token format consists of four fields, as shown in Figure 1–8. The starting delimiter indicates the initial boundary of a transmission sequence. The frame control field defines the frame type, and the ending delimiter indicates the end of the transmission.

NOTE: Sniffer Versions 4.5 and earlier do not capture FDDI tokens.

Preamble	Starting Delimiter	Frame Control	Ending Delimiter
16 or more symbols	2 symbols	2 symbols	2 symbols

Figure 1–8. Token Frame Format for FDDI

Format of a Data Frame

The FDDI frame format is similar to the IEEE 802 frame format, and is shown in Figure 1–9. The frame starts with a preamble and a unique starting delimiter octet, followed by the frame control (FC) octet. The FC octet determines whether the frame is an SMT frame, a MAC frame, a synchronous LLC frame, or an asynchronous LLC frame. Following the data field is a frame check sequence that checks the validity of all previous data, and an ending delimiter. The last octet for data frames is the frame status byte, containing bits that may be set by active stations on the ring.

Preamble	Starting Delimiter	Frame Control	Destination Address	Source Address	Data	Frame Check Sequence	Ending Delimiter	Frame Status
8 or more octets	1 octet	1 octet	2 or 6 octets	2 or 6 octets		4 octets	1 or 2 symbols	3 or more symbols

Figure 1–9. Data Frame Format for FDDI

Station Management

The Station Management (SMT) standard defines the station level controls necessary to manage a station on an FDDI network. SMT contains these components:

- Connection management (CMT) connects nodes to the FDDI network, manages physical connection between adjacent PHYs, configures PHY and MAC entities within a node, and coordinates trace functions.
- Ring management (RMT) receives status information from MAC and CMT and reports this status to SMT and higher-level processes.
- SMT frame services provide the means to control and observe the FDDI network.

See the discussion of the SMT protocol interpreter suite in Chapter 2 for more details concerning station management.

WAN/Synchronous Architecture

Synchronous data communications are used locally (as, for example, on a simple RS-232C link between computers in the same building) and also for communication over wide area networks (WANs). WANs, in turn, are being used increasingly in support of internetworking — connecting local area networks (LANs) together by means of WAN links. Most internetworking is currently done over leased lines using some variation of HDLC-like protocols. The Frame Relay protocol (described in Chapter 2) is frequently used to forward LAN frames over WAN links. Some implementations use the X.25 protocol (also described in Chapter 2) over HDLC.

At the network layer, X.25 defines a general purpose interface between data terminal equipment (DTE) and data circuit-terminating (or communications) equipment (DCE). A DTE is an end-user machine. The entry point to the WAN is a DCE.

At the logical link level, the International Organization for Standardization (ISO) published the widely used standard, High-level Data Link Control (HDLC) protocol. There are several important protocol subsets of the HDLC superset. Link Access Procedure Balanced (LAPB) supports the widely accepted X.25 packet network protocol. Synchronous Data Link Control (SDLC) is IBM's version of HDLC and is used for its Systems Network Architecture (SNA) protocol. Finally, LLC is the standard released by the IEEE 802 standards committee for LANs (See the discussion of "LLC Frames" in "Ethernet Network Architecture" on page 1–1).

Several standards have been implemented at the lower layers of the synchronous architecture and allow users a wide range of options to interface to a packet-switched network. Physical layer standards include the Electrical Industries Association's familiar RS-232C. The International Consultative Committee for Telephony and Telegraphy (CCITT) defined two well-known sets of standards, the V-Series (V.35, for example) and the X-Series (X.21, for example). Several of these other standards are related to RS-232C: CCITT V.24 and V.28, CCITT X.21bis, and ISO 2110.

Interconnection and Speed

Typically, RS-232C specifies a 25-pin connector, so that up to 25 wires can be used to connect two devices. The electrical characteristics of RS-232C place a limit of about 50 feet on the distance between, for example, a DTE and its modem. These same characteristics limit the data transmission rate across the interface to a maximum of about 19.2 Kbps.

V.35 allows data transmission at higher speeds (56 Kbps to 1.54 Mbps in the US; 64 Kbps to 2.048 Mbps internationally). It is implemented using both the frequency modulation and amplitude modulation techniques. The Sniffer analysis application's connection to V.35 is baseband.

Format of a Frame

Frames captured from a synchronous line and interpreted by the Sniffer Internetwork Analyzer generally conform to the HDLC standard defined by ISO. In particular, two subsets of HDLC are relevant to Sniffer Internetwork Analyzer users — SDLC and LAPB. The Sniffer analysis application will also recognize proprietary versions of HDLC framing implemented by Wellfleet, Cisco, Vitalink, Proteon, IBM, and Point-to-Point (PPP), as well as Frame Relay formats conforming to the ANSI standard or to RFC 1490.

SDLC is IBM's version of the HDLC superset. It is the logical link layer protocol for IBM's network layer services of its SNA protocol. LAPB is the link layer protocol for the network layer protocol X.25. Sniffer menus and screens refer to LAPB as HDLC.

One major difference between LAPB and SDLC involves the stations' responsibilities and the rules that the stations follow when transferring information. LAPB stations, like LLC stations, allow any station to initiate transmissions without prior permission from any other station (referred to as *Asynchronous Balanced Mode* or ABM). SDLC, on the other hand, requires a subservient *secondary* station to receive explicit permission from a dominant *primary* station before transmitting (referred to as *Normal Response Mode* or NRM). Unlike the *balanced* configuration of LAPB stations where stations are equally responsible for the link, the SDLC station configuration is *unbalanced*—the prime responsibility for the link depends upon the primary station.

Both LAPB and SDLC conform to the general HDLC frame format. The format of each frame is shown in Figure 1–10.

Flag: *1 byte*	**Address:** *1 byte*	**Control:** *1-2 bytes*	**Information:** *variable*	**FCS:** *2 bytes*	**Flag:** *1 byte*

|◄— **Recorded by the Sniffer Analyzer** —►|

Figure 1–10. The General HDLC (Including LAPB and SDLC) Frame Format

The **flag** is a special bit sequence, 01111110, that indicates either the beginning or the end of a frame. A technique known as "bit stuffing" is used to ensure that occurrences of this bit pattern in the frame data are not misinterpreted as

flags. The transmitting machine checks between the opening and closing flags, and it inserts a 0 bit when it encounters five consecutive 1 bits. After the frame has been "stuffed" and flags placed, the transmitting machine sends the frame to the receiver. The receiver monitors the bit stream. Whenever the receiver encounters six consecutive 1 bits, it knows that it has received a flag. Otherwise, when it sees five consecutive 1 bits followed by a 0, it removes that 0.

The **address** field identifies the primary or the secondary station transmitting a particular frame. Each station has a unique address. In unbalanced configurations, address fields contain addresses of secondary stations in both commands and responses. In balanced configurations, command frames contain the destination address, and response frames contain the transmitting station address.

The **control** field defines the exact function of LAPB and SDLC frames using the general HDLC frame format. It performs various functions, depending upon whether a frame is an *Information, Supervisory*, or *Unnumbered* frame (see below).

There are two important differences between LAPB and SDLC frames with regard to the control field:

- One is that each type of configuration has its own mode-setting command to establish link-level contact as either balanced or unbalanced.
- The other difference is that in the balanced configuration of LAPB, all stations can send commands and responses. In the unbalanced configuration of SDLC, a frame sent by a primary station is a command, and a frame sent by a secondary station is a response.

The three HDLC frame types are described below:

Information

I frames are used to convey or acknowledge end-user data between two devices. The control field of this type of frame contains both a *send sequence number* N(S) for itself and a *receive sequence number* N(R) for the next frame expected from the other station.

Supervisory

S frames are used to control the flow of data. The control field of this frame type contains an N(R) number but not an N(S) number. In addition, the control field contains the indications listed in Table 1–3 as either a command or a response.

Table 1–3. Commands and Responses Used in HDLC (SDLC and LAPB) Supervisory Frames

Command/Response	Action
RR	*Receive Ready.* I frame transmission and/or acknowledgment can proceed.
RNR	*Receive Not Ready.* I frame transmission and acknowledgment are blocked.
REJ	*Reject.* Retransmission starting with N(R) number is requested.

Unnumbered

U frames are also used for control purposes. The control field of this frame type contains neither N(S) nor N(R) numbers but may contain control information or data. The commands and responses appearing in the unnumbered frame control field are listed in Table 1–4.

Table 1–4. Commands and Responses Used in HDLC (SDLC and LAPB) Unnumbered Frames (1 of 2).

Command/Response	Action
SNRM	*Set Normal Response Mode.* Configure a secondary station in a mode that precludes it from sending unsolicited frames. The primary station controls all message flow. Used in SDLC.
SNRME	*Set Normal Response Mode (Extended).* Same as SNRM except that it selects modulo 128 sequence numbering rather than modulo 8 sequence numbering.
SABM	*Set Asynchronous Balanced Mode.* Configure stations as peers with each other. Used in LAPB.
SABME	*Set Asynchronous Balanced Mode (Extended).* Same as SABM except that it selects modulo 128 sequence numbering rather than modulo 8 sequence numbering.
DISC	*Disconnect.* Command used to place a secondary station in the disconnected mode (not operational).
DM	*Disconnected Mode.* Used by secondary station to indicate that it is in the disconnected mode.

Table 1–4. Commands and Responses Used in HDLC (SDLC and LAPB) Unnumbered Frames (2 of 2).

Command/Response	Action
UA	*Unnumbered Acknowledgment.* Response to set mode commands and to DISC.
FRMR	*Frame Reject.* The format of a received frame was invalid. The information field contains the reason.
XID	*Exchange Identification.* Used between two stations to exchange identification and the characteristics of the two stations.
UI	*Unnumbered Information.* Used for transmission of user data in an unsequenced frame.

The only HDLC Frames that are allowed to contain data after the header are I, UI, TEST, XID, and FRMR Types.

Phases of Link Control

The following five phases represent the fundamental sets of activities on a synchronous line using HDLC (SDLC and LAPB):

Connect Phase

Establishes a connection over a switched facility. The process includes off-hook signaling, switching, and exchange of identification.

Link Establishment Phase

Typical processes in this phase include initializing data transfer (over an already established physical link) and polling.

For example, when a DCE is able to proceed with a connection, it sends DISC frames with the *Poll* bit set *on*. When a DTE wants to reconnect to the DCE, it waits until it receives a DISC frame and then responds with a UA frame with the *Final* bit set on. The DCE is responsible for setting up the link when it receives the UA frame within the required amount of time. The specific link setup command depends upon the HDLC subset in use: if it is LAPB, the commands are SABM and SABME; if it is SDLC, the commands are SNRM and SNRME. After the DCE receives the link setup command in the required amount of time, it responds with a UA frame, and the link is now in an "up" state.

Information Transfer Phase

The information transfer phase follows link establishment. It includes the acknowledgment process as well as the actual data transfer between connected stations.

For example, the DTE sends an **I** frame. The DCE may acknowledge with either an **RR** frame or another **I** frame (if it too has data to send), and it may delay acknowledgment. When the DCE does acknowledge, it sends an N(R) number that is inclusive of all traffic transmitted and accepted.

Termination Phase

The termination phase relinquishes control of the link following transmission of data. In an unbalanced configuration, the secondary station returns control to the primary station.

Clear Phase

The clear phase releases the facility. For example, the DTE sends a DISC frame to tear down a link. The DCE responds by transmitting a UA frame.

ISDN Network Architecture

ISDN is a dial-up digital network service that provides digital transmission of images, voice, and data on the same physical line. ISDN can be thought of as a digital "pipe" between the telephone company and the ISDN subscriber. The ISDN pipe carries a number of different communication *channels*. The two major types of channels are:

B Channels

The B channel (or, the *bearer* channel) is a user channel that can carry digital data, digital voice traffic, or a mixture of lower-rate traffic. There are no protocol restrictions for B channels — they are transparent, circuit-switched 64 Kbps connections.

D Channels

The D channel (or, the *call-signaling* channel) provides an out-of-band common channel signaling facility for ISDN. *Common channel signaling* is a signaling method in which a channel separate from the ones carrying user traffic (such as voice, data, and video) is used to carry call signaling information.

The D channel is the "traffic cop" for the B channels —it is used by the ISDN switch to set up connections, identify called and calling stations, identify line and network status, and provide billing information to the telephone company.

Figure 1–11 describes the functions of the B and D channels.

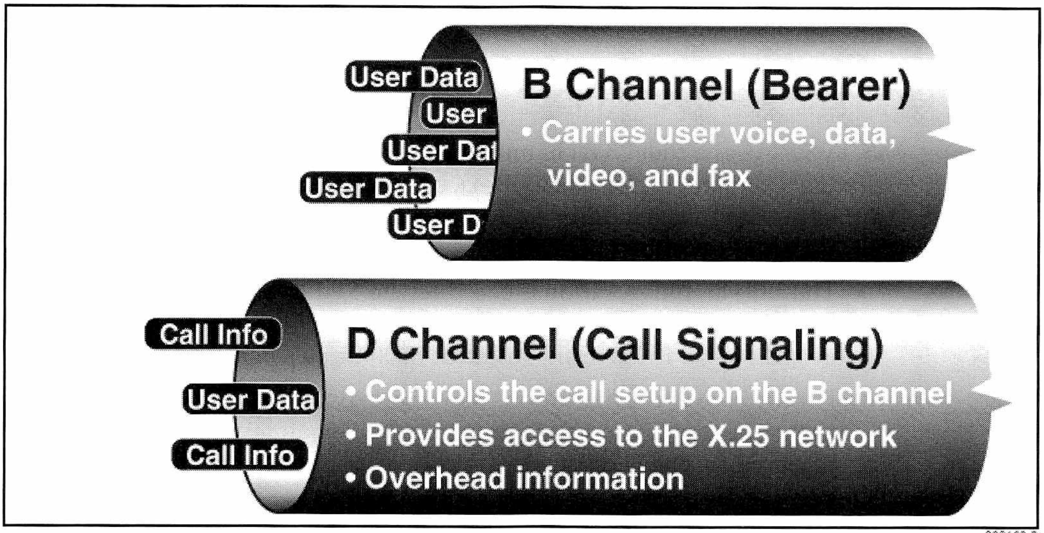


Figure 1–11. Functions of the B and D Channels in ISDN

Physical Interconnection and Speed

There are two major types of ISDN circuits:

- Basic Rate Interface (BRI) ISDN uses two B channels and one D channel (2B+D). The D channel for ISDN BRI is a 16 Kbps channel that is shared for signaling, small data transactions (such as credit card authorizations), and telemetry.
- Primary Rate Interface (PRI) ISDN uses either 23 B channels and one D channel (23B+D, or T1) or 30 B channels and one D channel (30B+D, or E1). The 23B+D configuration is used in the United States, Canada, and Japan, while the 30B+D configuration is used in Europe. In either case, the D channel for ISDN PRI is a 64 Kbps channel that is used exclusively for signaling.

The Basic Rate Interface "Pipe"

ISDN BRI uses two full-duplex 64 Kbps B channels and a full-duplex 16 Kbps D channel. The total bit rate is 144 Kbps.

An ISDN BRI installation can be either point-to-point or point-to-multipoint. In the point-to-point configuration, only one device is connected at the customer's premises. In a point-to-multipoint configuration, up to eight ISDN devices can be connected to the circuit at the customer's premises, each with

its own telephone number. Each connected device has access to the two 64 Kbps B channels and the 16 Kbps D channel provided by the ISDN BRI circuit.

The Primary Rate Interface "Pipe"

ISDN PRI uses either 23 B channels and one D channel (23B+D, or T1) or 30 B channels and one D channel (30B+D, or E1). Because different countries have different data rate standards, it is necessary to have two different types of ISDN PRI, as described below:

- The 23B+D configuration is based on the T1 data rate of 1.544 Mbps, which is standard in the United States, Canada, and Japan. This implementation uses a 193-bit frame transmitted at 8000 frames per second.

  For the 23B+D configuration, frames are divided into 24 timeslots of 8 bits each. The first 23 timeslots comprise the B channels, while Timeslot 24 is reserved for the D channel.

- The 30B+D configuration is based on the E1 data rate of 2.048 Mbps, which is standard in Europe. This implementation uses a 256-bit frame transmitted at 8000 frames per second.

  For the 30B+D configuration, frames are divided into 32 timeslots of 8 bits each. Timeslots 1 through 15 and 17 through 31 comprise the B channels, while Timeslot 16 is reserved for the D channel. Timeslot 0 is reserved for synchronization.

Figure 1–12 shows the primary rate interface "pipe" for a 23B+D configuration.

NOTE: In some ISDN PRI configurations, it is possible to have PRI with all B channels and no D channel for signaling. In this configuration, a D channel on another PRI at the same subscriber location provides the signaling.

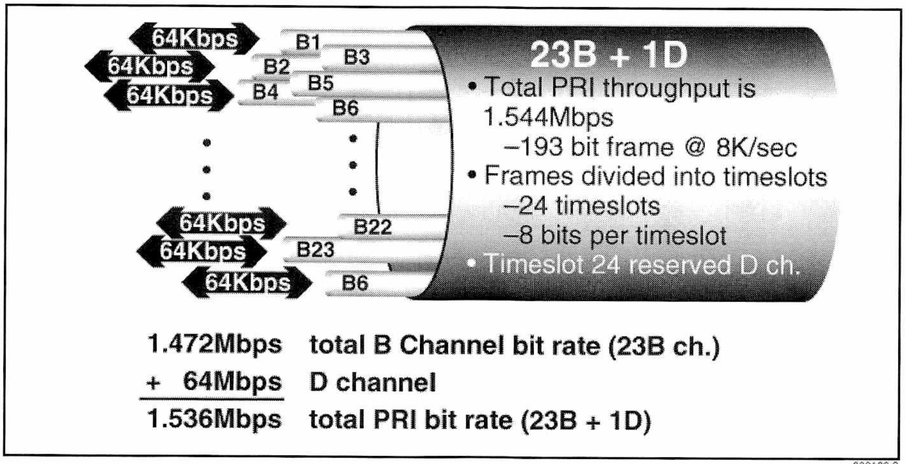


Figure 1–12. The Primary Rate Interface "Pipe" for a 23B+D Configuration

Common ISDN PRI Configuration

In an ISDN PRI implementation, only one device can have access to the ISDN circuit from the telephone company. This is known as a *point-to-point* configuration. In typical installations, the ISDN PRI subscriber will connect the ISDN circuit from the telephone company to a "front-end" ISDN bandwidth aggregator (or hub) that controls the PRI bandwidth. This device accepts communications from various user sources such as ISDN phones, video conference codecs, or a LAN, and provides bandwidth on demand. Figure 1–13 shows a typical implementation of ISDN PRI (in this case, a 23B+D configuration).

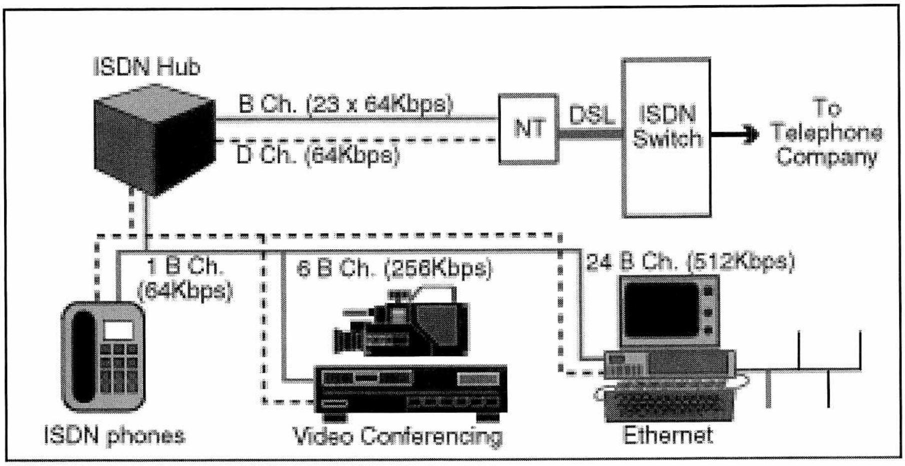


Figure 1–13. Typical Point-to-Point Implementation of 23B+D ISDN PRI

In Figure 1–13, the following terminology is used:

DSL Digital Subscriber Loop. The digital subscriber loop is the digital extension from the telephone company to the subscriber. In the case of 23B+D ISDN PRI, the digital subscriber loop is a T1 circuit. In the case of 30B+D ISDN PRI, the digital subscriber loop is an E1 circuit.

NT Network Termination. The primary purpose of the NT is to terminate the digital circuit from the telephone company. In addition to terminating the PRI circuit, the NT also provides low-level line conditioning. Because ISDN PRI can be thought of as ISDN over either T1 or E1, the NT closely resembles a Channel Service Unit (CSU).

Signaling and Link Access in ISDN

In ISDN (either BRI or PRI), signaling and control of access to the B channels in handled on the D channel. All traffic over the D channel uses a link layer protocol called the Link Access Protocol-D (LAP-D). LAP-D is modeled after the LAP-B protocol used in X.25 and HDLC (see "WAN/Synchronous Architecture" on page 1–20 for information on LAP-B, X.25, and HDLC).

LAP-D is the data link layer (Layer 2) protocol for the Layer 3 signaling protocol, Q.931. It is used to convey information between signaling entities across the ISDN. In turn, Q.931 is the network layer (Layer 3) signaling

protocol used to establish, maintain, and tear down connections on the B channels of the ISDN. Q. 931 is similar to X.25 in operations — both are Layer 3 protocols used to establish logical connections.

Table 1–5 illustrates the relationship of D channel services to the OSI model. The ITU recommendation defining the exact services provided at each layer is also listed.

Table 1–5. How D Channel Services Relate to the OSI Model

At this OSI Layer...	This D channel service...	Provides these functions...	And is similar to this standard.
Layer 3 Network Layer	Q.931 (I.450, I.451)	Signaling information used to set up, maintain and tear down connections on the B channels.	X.25
Layer 2 Data Link Layer	LAP-D (I.441)	Provides for exchange of Layer 3 information across the ISDN.	HDLC, LAP-B
Layer 1 Physical Layer	BRI (I.430) PRI (I.431)	Defines physical characteristics of link.	

ATM Network Architecture

Asynchronous Transfer Mode (ATM) is a cell-based switching and multiplexing network technology that is designed to be flexible and scalable in nature. This way, ATM can provide support for a wide range of services, from traditional IP packet data to video and imaging services.

There is no single standard for ATM — it is a technology defined by protocols standardized by the following organizations:

- ITU-T
- ANSI
- ATM Forum

The fundamental unit in ATM is the *cell*. ATM defines a fixed-length cell of 53 bytes as its fundamental transmission unit. Each cell consists of 5 bytes of header information and 48 bytes of payload. Figure 1–14 shows this.

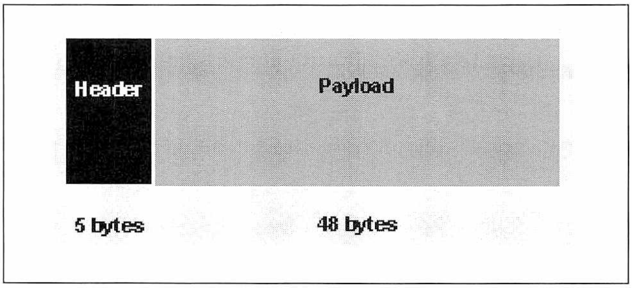


Figure 1–14. ATM Cell — An Overview

Cells are transmitted in a continuous stream over a supported physical transmission path, such as the North American SONET standard, the European E1 standard, or the ITU-T STM standards (see "Physical Interconnection and Speed" on page 1–33 for more information). In an ATM network, all data is switched and multiplexed in these 53-byte cells.

The B-ISDN Protocol Stack

ITU-T Recommendation I.321 is a good starting point for a discussion of ATM. It defines the B-ISDN protocol stack which is the foundation for ATM. The B-ISDN protocol stack defined in ITU-T I.321 is used as the reference point to structure all further ITU-T recommendations for ATM.

ITU I.321 divides the B-ISDN stack into four basic layers: the Physical layer, the ATM layer, the ATM adaptation layers (AAL) and higher layers. However, some of these layers are sublayered extensively. Table 1–6 provides an overview of the B-ISDN protocol stack and the services provided at each layer.

Table 1–6. Services Provided by Major Layers in B-ISDN Protocol Model

This layer...			does the following in the ATM (B-ISDN) protocol model..
Higher Layers			Provides higher layer services on top of ATM, such as IP, LAN Emulation, Frame Relay, and so on.
ATM Adaptation Layer (AAL)	**Convergence Sublayer (CS)**	**Common Part (CS) Sublayer**	Adapts the services provided by the ATM layer to those required by higher layers, such as circuit emulation, packet video, or Frame Relay.
		Service Specific (SS) Sublayer	
	SAR Sublayer		
ATM Layer			Provides for cell construction, cell relaying using the VPI/VCI, cell loss priority processing, processing of reserved header types (for management cells, for example), and generic flow control, among others.
Physical Layer	**Transmission Convergence (TC) Sublayer**		Provides for the conversion between ATM cells and the clocked bitstream required by the PMD. Includes cell rate decoupling (inserting empty cells into the bitstream when there is no data to send), and cell delineation (finding the boundaries between cells)
	Physical Medium Dependent Sublayer		The PMD takes care of the actual transmission of the bits in the ATM cells. The usual physical layer services are found here, such as bit timing and line encoding.

Physical Interconnection and Speed

The physical layer provides for the transmission of ATM cells over a physical medium that connects two ATM devices. The physical layer in the ATM B-ISDN protocol model is divided into the Physical Medium Dependent (PMD) and Transmission Convergence (TC) sublayers. The TC sublayer takes the cells from the ATM layer and turns them into a bitstream suitable for transmission over the PMD. The PMD sublayer provides the actual transmission of the bits in the ATM cells.

There are a variety of transmission speeds and physical mediums defined for ATM. The speeds and physical mediums defined by the ATM Forum are listed in Table 1–7.

Table 1–7. Speeds and Mediums for ATM as Defined by the ATM Forum

Medium	Speeds
Multimode Fiber	155 Mbps, SONET STS-3c
	100 Mbps, 4B/5B coding
	155 Mbps, 8B/10B coding
Single Mode Fiber	155 Mbps, SONET STS-3c
Shielded Twisted Pair (Copper)	155 Mbps, 8B/10B Coding
Coaxial Cable	45 Mbps, DS3

In addition to the ATM Forum, both ANSI and the ITU-T have defined supported speeds for ATM. Fortunately, the standards agree.

ANSI standard T1.624 defines the following SONET-based speeds for ATM:

- STS-1 at 52 Mbps
- STS-3c at 155 Mbps
- STS-12c at 622 Mbps

ANSI standard T1.624 also defines the DS3 rate of 45 Mbps using the Physical Layer Convergence Protocol (PLCP).

For Europe, ITU-T recommendation I.432 defines physical interfaces for ATM which correspond to the ANSI and ATM Forum rates. These include:

- STM-1 at 155 Mbps
- STM-4 at 622 Mbps

Notice that STM-1 and STM-4 correspond exactly to the STS-3c and STS-12c rates defined by ANSI. The ITU also defines physical interfaces for ATM corresponding to the following rates:

- E1, E3, and E4 rates.
- DS1, DS2, and DS3 rates.

Format of a Cell

The ATM layer is at the heart of ATM technology. It is responsible for constructing cells, addressing cells using the VPI and VCI identifiers, and making sure cells get to their proper destinations.

Recall that each ATM cell is fixed at 53 bytes long — 5 bytes of header and 48 bytes of payload. Figure 1–15 provides a detailed look at each of the fields in the ATM User-Network Interface (UNI) cell. The top row of the table lists each bit within a cell by number.

<table>
<tr><td>7</td><td>6</td><td>5</td><td>4</td><td>3</td><td>2</td><td>1</td><td>0</td><td rowspan="6">5 bytes</td></tr>
<tr><td colspan="4">Generic Flow Control</td><td colspan="4">Virtual Path Identifier</td></tr>
<tr><td colspan="4">Virtual Path Identifier</td><td colspan="4">Virtual Channel Identifier</td></tr>
<tr><td colspan="8">Virtual Channel Identifier</td></tr>
<tr><td colspan="4">Virtual Channel Identifier</td><td colspan="3">Payload Type Identifier</td><td>CLP</td></tr>
<tr><td colspan="8">Header Error Check</td></tr>
<tr><td colspan="8">Payload
(48 bytes)</td><td>48 bytes</td></tr>
</table>

CLP = Cell Loss Priority

Figure 1–15. Format of an ATM Cell — Detail

The next sections discuss each of the fields in the ATM UNI cell and how they are used.

Virtual Paths and Virtual Channels

The Virtual Path Identifier and Virtual Channel Identifier are used to get cells from place to place. Together, they form the destination address of a cell and are used for switching. The combination of VPI/VCI values is used by the ATM network to associate a particular cell with a particular connection between two ATM endpoints.

A virtual path is like a bundle of virtual channels. Since the VPI is 8 bits, on any given interface, there can be up to 256 different bundles of VCIs. The advantage of this is that VCIs can be reused within a VPI.

The Cell Loss Priority (CLP) Bit

The CLP bit is used by the ATM network to determine what cells should be discarded during periods of congestion or heavy network activity. Cells with the CLP bit set to "true" will be discarded before cells without the CLP bit set.

Each connection on the ATM network has a traffic contract. The key to the traffic contract is the Cell Loss Priority (CLP) bit, included in every ATM cell. Cells with the CLP bit set can be thought of as expendable—they are to be discarded by the network before cells that do not have the CLP bit set. The ATM network watches the cells on a connection to make sure they do not violate the traffic contract. If a cell does violate the traffic contract for a connection, the network sets its CLP bit, making it eligible for discarding if the network begins to experience congestion.

The traffic contract is based on the "leaky bucket" algorithm, as defined in the ATM Forum's UNI Specification, Version 3.1, or CCITT Recommendation I.371. The leaky bucket algorithm uses the descriptors and tolerances found in the ATM Traffic Descriptor information element (such as peak cell rate, sustainable cell rate, and so on) to define the traffic contract for a connection. Refer to the reference documentation listed above for details.

The Payload Type Identifier

The payload type identifier is a three-bit field used to distinguish between cells carrying user information and cells carrying management information. The payload type identifier can indicate different types of Operations and Management (OAM) cells, as well as different types of Explicit Forward Congestion Indication (EFCI) cells.

The Generic Flow Control (GFC) Field

The GFC field is found in the first four bits of the header. It is currently undefined, but may be used later for flow control.

NOTE: NNI cells do not use the GFC field. It is only present in UNI cells.

The Header Error Check (HEC) Field

The HEC field is found in the last eight bits of the header. It is used to validate the VPI/VCI values of a cell. The HEC can be used in two ways:

- In **Detection mode**, cells are discarded when a header error is detected.
- In **Correction mode**, the headers of cells with one-bit errors can be corrected. Cells with headers that exhibit multiple-bit errors are discarded.

Note that the HEC field is also used by SONET (at the physical layer) for cell delineation.

The ATM Adaptation Layer (AAL)

The AAL adapts the services provided by the ATM layer to those required by higher layers, such as circuit emulation, packet video, or Frame Relay.

There are different types of AAL depending on the type of service to be provided on a given connection. The ITU-T has defined bearer classes to classify the various kinds of services that might be carried over ATM. These service classes are used as guides to defining AAL protocols. Service classes are defined according to end-to-end timing requirements, bit rates, and connection modes. Table 1–8 shows the different bearer classes defined by the ITU-T's Recommendation I.362, along with an example of each.

Table 1–8. Bearer Classes Defined by ITU-T Recommendation I.362

	Class A	Class B	Class C	Class D
End-to-end timing	Required		Not required	
Bit rate	Constant	Variable		
Connection mode	Connection-oriented			Connectionless
Example	64 Kbps voice	Variable bit rate video	Connection-oriented data transfer over ATM (such as Frame Relay)	Connectionless data transfer over ATM (such as IP).

- AAL 1 is used for Class A traffic.
- Although still under development, AAL2 will be used for Class B traffic.
- Both AAL 3/4 and AAL 5 are used for Class C and Class D traffic.

Quality of Service (QoS) Parameters and Bearer Classes

Each ATM connection has a traffic contract that specifies (among other things) the QoS that the network is expected to provide for that connection. Each QoS class corresponds to a Bearer Class defined by the ITU-T (see Figure 1–8). QoS is defined by allowable cell loss and cell delay. A Class 1 QoS provides the best service (that is, the least amount of cell loss and cell delay) while a Class 4 QoS provides the worst. Table 1–9 summarizes the various QoS classes defined by the ATM Forum.

Table 1–9. QoS Classes Defined by the ATM Forum

QoS Class	QoS Parameters	Applications
0	Unspecified	“Best effort,” or “at risk.”
1	Specified	Meets Bearer Class A requirements. Used for 64 Kbps digital voice applications, circuit emulation.
2	Specified	Meets Bearer Class B requirements. Used for variable bit rate packetized video and audio.
3	Specified	Meets Bearer Class C requirements. Used for connection-oriented data protocols, such as Frame Relay.
4	Specified	Meets Bearer Class D requirements. Uses for connectionless data protocols, such as IP or SMDS.

Chapter 2
Major Protocol Suites

Overview

Following a brief introductory section on the Open Systems Interconnection (OSI) layered protocol model, this chapter provides general information on each of the major protocol suites interpreted by Network General's Sniffer analysis application. The information includes a short discussion of the suite itself, a diagram that maps each protocol to the OSI model, and a summary of the services provided by each protocol.

Introduction

The Sniffer analysis application does not simply monitor, capture, or record network traffic. It also interprets what it records. Protocol interpretation is what makes the Sniffer analysis application a valuable tool. Interpretation turns an inscrutable stream of bits and bytes into clearly labeled commands, responses, and readable text.

Interpretation routines are an integral part of the Sniffer analysis application software, built-in at the factory during a process that equips each machine for the network requested by the customer. Network General calls the interpretation routines *protocol interpreters* (PIs). The interpretation they do covers the full range of the OSI seven-layer model (Figure 2–1).

Application	**Layer 7 is concerned with the support of end-user application processes.**
Presentation	**Layer 6 provides for the representation of the data.**
Session	**Layer 5 performs administrative tasks and security.**
Transport	**Layer 4 ensures end-to-end, error-free delivery.**
Network	**Layer 3 is responsible for addressing and routing between networks.**
Logical Link / *MAC* — *Data Link*	**Layer 2 is responsible for the transfer of data over the channel.**
Physical	**Layer 1 handles physical signaling, including connectors, timing, voltages, and other matters.**

Figure 2–1. Layers of the OSI Network Model

At the *physical* layer, the analyzer's hardware is responsible for sending and receiving network signals. For the *logical link* layer, interpreters are included to match the networks on which the analyzer will be used.

The protocols at the higher layers—*network, transport, session, presentation, application*—are largely independent of the physical layer.

IBM Protocol Interpreter Suite

The Sniffer analysis application interprets frames in four families of higher-level protocols widely used on IBM networks. While IBM uses these protocols on LANs connected by token ring, they may also be found on networks connected by other media. The IBM PI suite (Figure 2–2) is installed in a Sniffer analysis application equipped for connection to a LAN such as token ring, Ethernet, or to a wide area network's WAN/synchronous link by way of an RS-232 or V.35 interface.

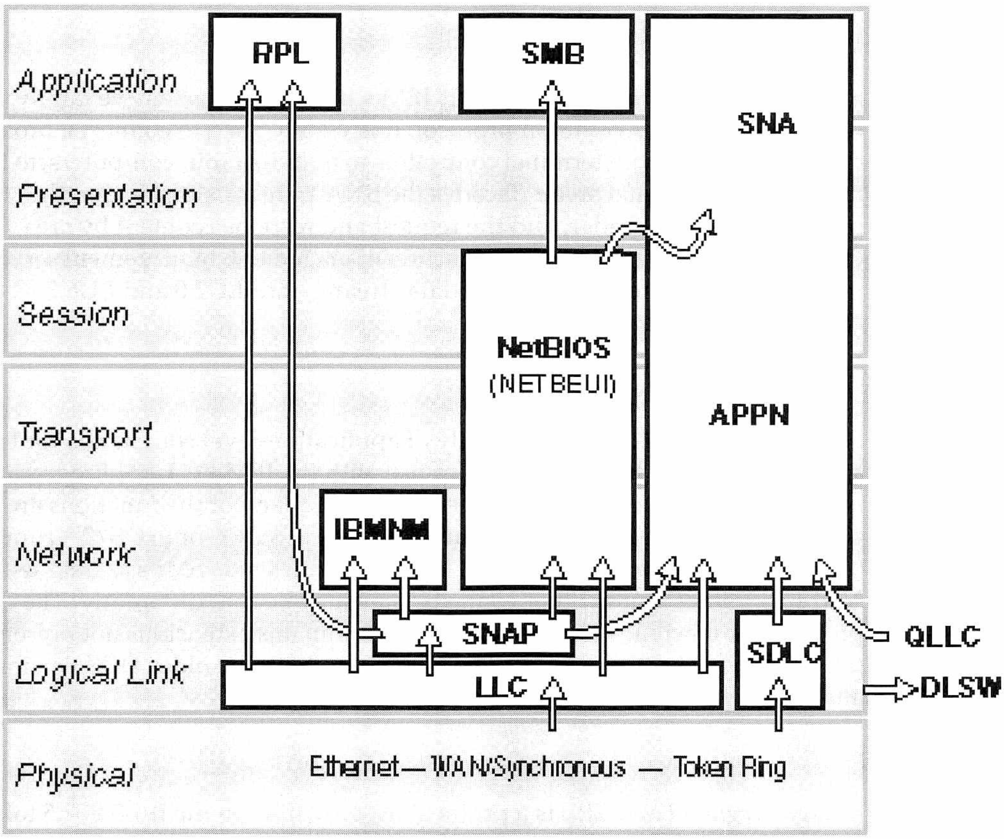


Figure 2–2. The IBM PI Suite Related to the OSI Reference Model

Protocols Interpreted

APPN

Advanced Peer-to-Peer Networking. APPN is second-generation Systems Network Architecture (SNA). APPN extends SNA to environments without mainframes, where midrange processors need to communicate as peers. Connections are peer-to-peer, so that any user can connect to any other user without mainframe involvement. Network administration is simpler, because APPN can dynamically create directories and routing information.

SNA

Systems Network Architecture. SNA is IBM's name for its extensive family of commands within a common protocol. It is widely used to connect a broad range of devices, from terminal controllers to micro- or minicomputers, to IBM mainframes. The interpreter decodes the SNA transmission header, the request/response header, and the request and response content by area, including transmission services, function management, management services, presentation services, and general data stream. Both LU2.0 and LU6.2 commands are decoded.

SMB

Server Message Block. SMB is a family of application-level commands for LAN servers developed by Microsoft® for use with the IBM PC LAN Program but frequently used in other environments as well. Many of the functions are similar to those made by an application program to DOS or to OS/2® running on a single computer. The IBM PC LAN Program sends SMBs as data within NetBIOS frames, but in other contexts, they may be sent differently. The SMB protocol for machines running under OS/2 contains extensions not present in the version for DOS machines. The PI decodes both the older DOS versions and the extended OS/2 versions.

RPL

Remote Program Load. RPL is a protocol used by IBM on the IEEE 802.5 token ring network to download initial programs into networked stations.

NetBIOS

Network Basic I/O System. NetBIOS is a protocol implemented in the IBM PC LAN Program to support communication between symbolically named stations and the exchange of arbitrary data between symbolically named stations. (Some of the other NetBIOS implementations differ from the IBM version. The NetBIOS module of the IBM PI suite differs accordingly from the corresponding NetBIOS modules of Novell NetWare® and TCP/IP.)

IBMNM

IBM Network Management Protocols (LLC SAP F4). IBMNM is used for the LAN Reporting Mechanism, Ring Error Monitor, Configuration Report Server, Ring Parameter Server, and LAN Bridge Server.

LLC

Logical Link Control (IEEE 802.2). LLC is a protocol that provides connection control and/or multiplexing to subsequent embedded protocols.

SDLC

Synchronous Data Link Control. SDLC is IBM's version of the logical-link layer protocol whose ISO designation is HDLC. The WAN/Synchronous Sniffer analysis application (Sniffer Internetwork Analyzer) interprets the subset that provides link-level support for X.25 and SNA.

Novell NetWare Protocol Interpreter Suite

The Sniffer analysis application interprets the protocols used by Novell's NetWare family of products, which include an operating system for file servers as well as services in support of remote users on a variety of physical media. The interpreter suite is installed on Sniffer systems for Ethernet, fast Ethernet, token ring, WAN/synchronous, FDDI, or ATM.

Each NetWare file server runs directly under a proprietary Novell operating system. Users at DOS or OS/2-based workstations can redirect their operating system functions to the NetWare servers. What Novell calls Network File Services (NFS) makes use of NetWare Core Protocol (NCP) to transmit commands or inquiries from workstations and to receive replies from file servers. NCP in turn makes use of Novell's implementation of the XNS family of protocols developed by Xerox. These protocols are concerned with the transmission and delivery of a packet, but not its interpretation, which is left to the higher-level protocol, NCP.

At the network level, NetWare uses a datagram protocol called IPX that corresponds to Xerox's IDP (Internet Datagram Protocol). Each IPX packet identifies the network, node, and socket of its destination and of its source. A socket may be a function within a node and, hence, affects where the embedded NCP message is interpreted.

NetWare also provides a connection-oriented virtual circuit protocol called SPX (Sequential Packet Exchange) that corresponds to SPP in the XNS protocols. (However, NCP provides connection services without the use of SPX packets.) In SPX, each packet is identified in the same way as an IPX packet, but with additional fields for the source and destination connection, a sequence number within that connection, an acknowledgment number, and an allocation of the number of unacknowledged SPX packets the connection may tolerate.

Figure 2–3 shows the Novell NetWare PI suite related to the OSI reference model.

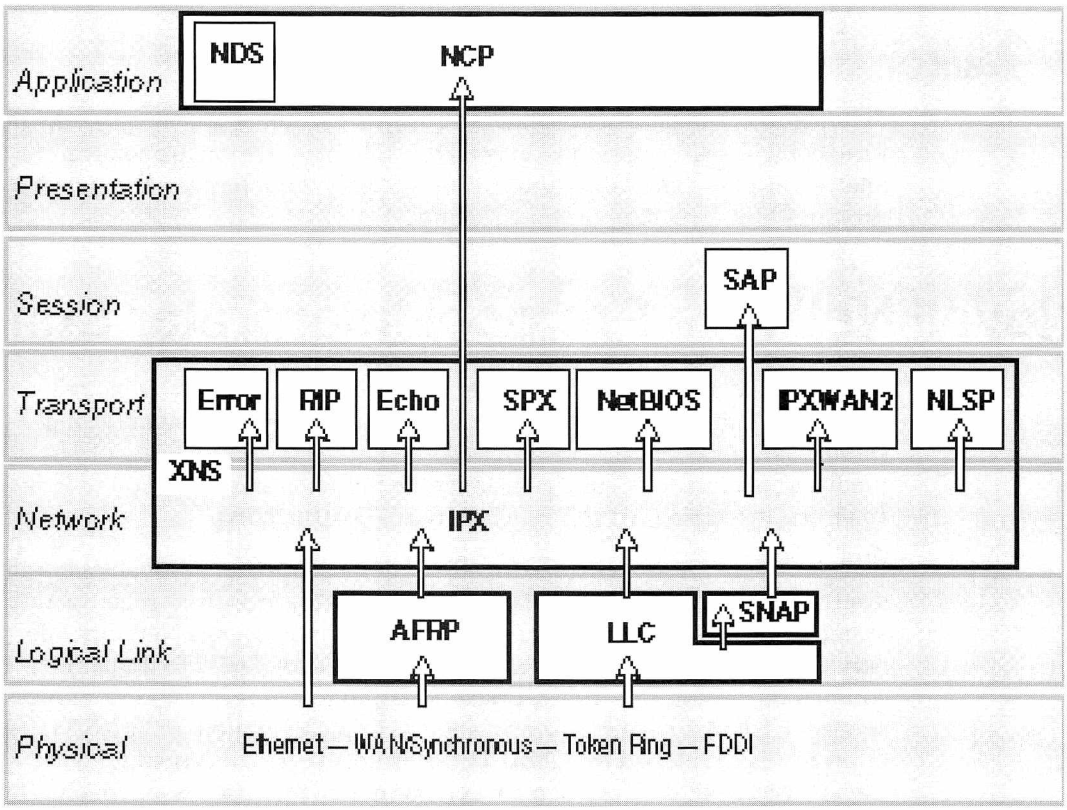


Figure 2–3. The Novell NetWare PI Suite Related to the OSI Reference Model

Protocols Interpreted

NCP

NetWare Core Protocol. NCP is a Novell application-level protocol for the exchange of commands and data between file servers and workstations; also described as NetWare File Service Protocol (NFSP).

NDS

NetWare Directory Services Protocol. NDS is a Novell protocol that operates with NCP to manage IPX routing.

NLSP

NetWare Link Services Protocol. NLSP is a link-state protocol that improves the performance, reliability, scalability, and manageability of IPX traffic in large-scale LAN-WAN internetworks.

SAP

Service Advertising Protocol. SAP is used by NetWare servers to broadcast the names and locations of servers and to send a specific response to any station that queries it.

NetBIOS

NetWare Basic I/O System. NetWare supports emulation of the protocol implemented by the IBM PC LAN Program to support communication between symbolically named stations and the exchange of arbitrary data. In the NetWare context, NetBIOS is atop IPX.

IPX

Internet Packet Exchange. IPX is a network-level protocol corresponding to Xerox IDP. Within this family of protocols, the following are identified:

- *SPX—Sequential Packet Exchange.* Novell's version of the Xerox transport-level protocol called SPP.
- RIP—*Routing Information Protocol.* Novell's version of a protocol used to exchange routing information among gateways.
- Echo—Request/response protocol used to verify the existence of a host.
- Error—A protocol by which a station reports that it has received (and is discarding) a defective packet.

AFRP

ARCNET Fragmentation Protocol. AFRP breaks up and reassembles network-layer packets so that they are acceptable to the data-link protocol and the underlying physical medium.

LLC

Logical Link Control (IEEE 802.2). LLC is a protocol that provides connection control and/or multiplexing to subsequent embedded protocols.

XNS Protocol Interpreter Suite

At the network, transport, and presentation layers, this PI suite handles the protocols of the Xerox Network System (XNS). After Xerox published the specifications of these protocols in 1981, several other vendors developed application-layer protocols that run on top of them. The XNS PI suite decodes SMB, a protocol used in Microsoft Networks (MS-NET™) and the IBM OS/2 LAN Manager™.

A network's upper-level protocols are largely independent of its physical layer. While Xerox developed XNS (Figure 2–4) for operation with Ethernet systems, XNS protocols may also be found on networks connected by other media. The XNS PI suite is installed in a Sniffer analysis application equipped for connection to Ethernet, fast Ethernet, token ring, WAN/synchronous, FDDI, or ATM.

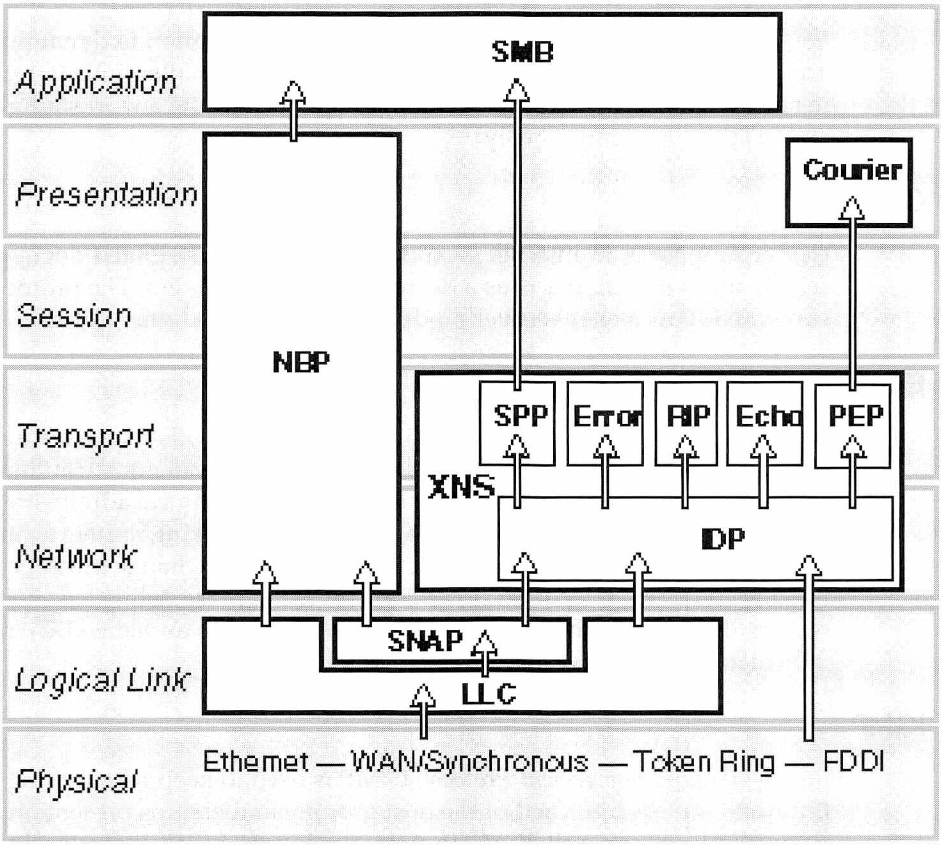


Figure 2–4. The XNS PI Suite Related to the OSI Reference Model

Protocols Interpreted

NNTP

Network News Transfer Protocol. NNTP is a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the ARPA-Internet community. It provides for the central-database storage of news articles and allows a subscriber to select and retrieve only a specified set of messages. Indexing, cross referencing, and expiration of aged messages are also provided.

POP3

Post Office Protocol - Version 3. POP3 permits a workstation to dynamically access a mail facility on a server host. This allows a smaller node to retrieve mail from the server host on demand without the need for a workstation to run an SMTP server continuously.

GOPHER

Gopher. Gopher is an Internet protocol designed for distributed document search and retrieval. It acts as a document delivery system. The protocol and software follow a client-server model on a TCP connection.

BGP

Border Gateway Protocol. BGP, as defined in RFC 1771, allows the creation of loop-free interdomain routing between autonomous systems. An autonomous system is a set of routers operating under a single technical administration. BGP uses TCP as its transport protocol. Two BGP-speaking routers form a TCP connection between one another (peer routers) and exchange messages to open and confirm the connection parameters. Peers are defined as any two routers that have formed a TCP connection in order to exchange BGP routing information. Peers may also be called neighbors.

IGMP

Internet Group Management Protocol. IGMP is used to keep neighboring multicast routers informed of the host group memberships present on a particular local network. IGMP is an integral part of IP. It is required to be implemented by all hosts conforming to level 2 of the IP multicasting specification. IGMP messages are encapsulated in IP datagrams, with an IP protocol number of 2. All IGMP messages of concern to hosts have the following format:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |Version| Type |     Unused      |
Checksum             |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                         Group
Address                         |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

EIGRP

Extended Interior Gateway Routing Protocol. EIGRP is an enhanced version of IGRP. It is a suite of Cisco routing protocols used in TCP/IP and OSI internets. It is considered to be an interior gateway protocol (IGP), but has also been used extensively as an exterior gateway protocol for interdomain routing.

NTP/SNTP

Network Time Protocol/Simple Network Time Protocol. NTP or SNTP provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet. It uses a returnable-time design in which a distributed subnet of time servers operating in a self-organizing, hierarchical master-slave configuration synchronize local clocks within the subnet and synchronize to national time standards via wire or radio. The servers can also redistribute reference time via local routing algorithms and time daemons.

Inverse ARP

Inverse Address Resolution Protocol. IARP allows a Frame Relay station to discover the protocol address corresponding to a given hardware address. It is more efficient than simulating a broadcast with multiple copies of the same message, and it is more flexible than relying on static configuration. IARP is an extension of the existing ARP, and has the same format as standard ARP.

IARP may be used in any network that provides destination hardware addresses without indicating corresponding protocol.

SMB

Server Message Block. SMB is a family of application-level commands for LAN servers developed by Microsoft and IBM for use with the IBM PC LAN Program but frequently used in other environments as well. Many of the functions are similar to those made by an application program to DOS or to OS/2 running on a single computer. Although the IBM PC LAN Program sends SMBs as data within NetBIOS frames, in other contexts they may be sent differently. The XNS PI suite decodes SMB frames transported by the Xerox IDP and SPP protocols. The SMB protocol for machines running under OS/2 contains extensions not present in the version for DOS machines. The XNS PI suite decodes both the older DOS versions and the extended OS/2 versions.

DVMRP

Distance Vector Multicast Routing Protocol. DVMRP is a protocol for routing multicast datagrams through an internet. It is derived from RIP (Routing Information Protocol). DVMRP is an interior gateway protocol suitable for use within an autonomous system, but not between different autonomous systems. DVMRP is not currently developed for use in routing non-multicast datagrams, so a router that routes both multicast and unicast datagrams must run two separate routing processes.

NBP

NetBIOS Protocol. NBP is used in 3Com 3+ Open software.

XNS

Xerox Network Systems Protocol. Within this family of protocols, the XNS PI suite interprets the following:

- *Courier*—A presentation-level protocol that delivers data to such application-level protocols as XNS Printing, XNS Filing, or XNS Clearinghouse (which the XNS PI suite identifies but does not interpret).
- *SPP—Sequenced Packet Protocol.* A virtual-circuit, connection-oriented protocol.
- IDP—*Internet Datagram Protocol.* Delivers to an internet address a single frame as an independent entity, without regard to other packets or to the addressee's response.
- *PEP—Packet Exchange Protocol.* Delivers a request and response pair; this protocol thus has a reliability greater than IDP alone, but less than achievable with SPP.
- *RIP—Routing Information Protocol.* Exchanges routing information among gateways and end systems.
- *Echo*—A request/response protocol used to verify the existence of a host.
- *Error*—A protocol by which a station reports that it has received (and is discarding) a defective packet.

TCP/IP Protocol Interpreter Suite

The Sniffer analysis application interprets the protocols of the TCP/IP family and other related protocols. TCP/IP was developed during the 1970's by research institutions under grants from the Advanced Research Projects Agency (ARPANET), U.S. Defense Department. Since its adoption as a standard for ARPANET in 1978, TCP/IP has become widely used in many other networks linking commercial or educational institutions. Although the U.S. Congress has mandated the eventual adoption of ISO protocols, TCP/IP is likely to remain widely used for some time.

While TCP/IP (Figure 2–5) usually runs on Ethernet, its protocols may also be found on other networks. The TCP/IP PI suite is installed in a Sniffer analysis application for Ethernet, fast Ethernet, token ring, WAN/synchronous, FDDI, or ATM.

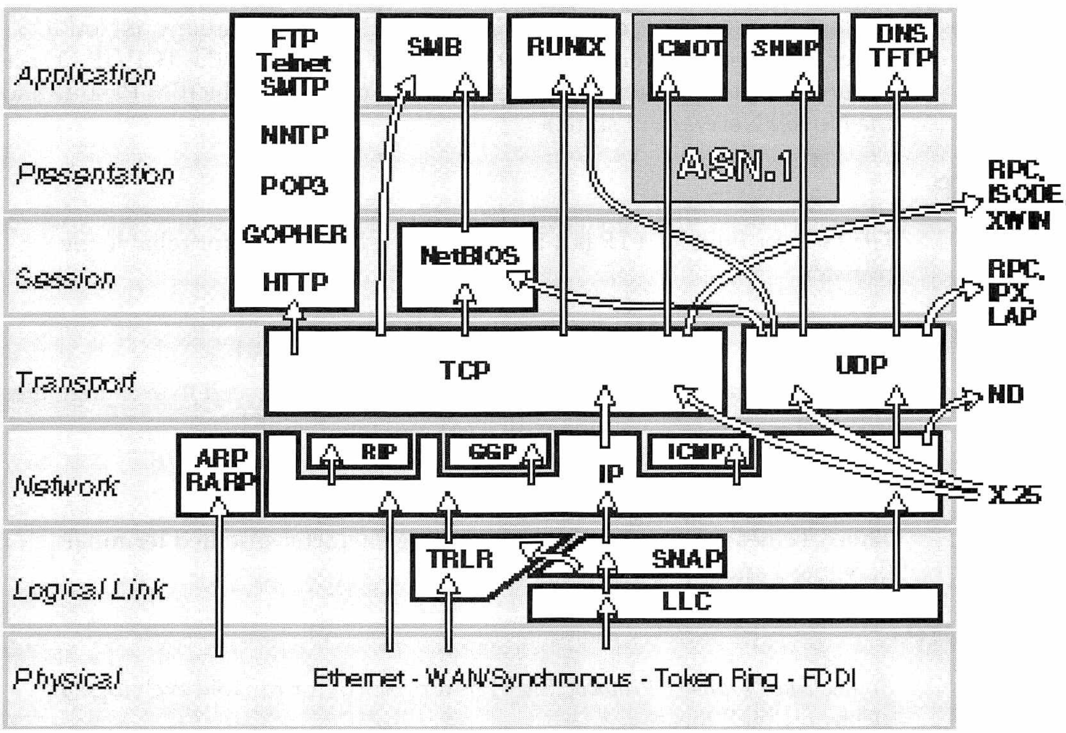


Figure 2–5. The TCP/IP PI Suite Related to the OSI Reference Model

Protocols Interpreted

SMB

Server Message Block. SMB is a family of application-level commands for LAN servers developed by Microsoft for use with the IBM PC LAN Program and frequently used in other environments. Although the IBM PC LAN Program sends SMBs as data within NetBIOS frames, in other contexts they may be sent differently. The TCP/IP PI suite decodes SMBs transported by TCP. The SMB protocol for machines running under OS/2 contains extensions not present in the version for DOS machines. The TCP/IP PI suite decodes both the older DOS versions and the extended OS/2 versions.

NetBIOS

Network Basic I/O System. NetBIOS is a TCP/UDP version of a protocol developed for the IBM PC LAN Program to support communication between symbolically named stations and transfer of arbitrary data. In the TCP/IP context, NetBIOS is over UDP or IP. (TCP/IP implementations of NetBIOS differ from the IBM version, and the NetBIOS module of the TCP/IP PI suite differs accordingly from the corresponding modules of the IBM PI suite and the Novell NetWare PI suite.)

FTP

File Transfer Protocol. FTP is a protocol based on TCP/IP for reliable file transfer.

TFTP

Trivial File Transfer Protocol. TFTP is a simple protocol used to exchange files between networked stations with less overhead than FTP.

Telnet

Telnet. Telnet is a protocol for transmitting character-oriented terminal (keyboard and screen) data.

SMTP

Simple Mail Transfer Protocol. SMTP is a protocol for reliable exchange of electronic mail messages.

RUNIX

Remote Unix. RUNIX is a protocol for handling remote requests to a UNIX host, including commands RLOGIN, RWHO, REXEC, RSHELL, and remote printing.

DNS

Domain Name Service. DNS is a protocol for finding information about network addresses using a database distributed among differently named servers.

TCP

Transmission Control Protocol. TCP is a connection-oriented byte-stream protocol that provides reliable end-to-end communication using datagrams sent over IP.

UDP

User Datagram Protocol. UDP is a protocol that transmits datagrams over IP.

IP

Internet Protocol. IP is a protocol that handles end-to-end forwarding and long packet fragmentation control.

RIP

Routing Information Protocol. RIP is a protocol that exchanges routing information among gateways and end systems.

GGP

Gateway-to-Gateway Protocol. GGP is a protocol that exchanges routing information among IP gateways.

ICMP

Internet Control Message Protocol. ICMP is a protocol that reports on difficulties in datagram transmission.

LLC

Logical Link Control (IEEE 802.2). LLC is a protocol that provides connection control and multiplexing to subsequent embedded protocols.

ARP

Address Resolution Protocol. ARP is a protocol that finds a node's DLC address from its IP address.

IARP

Inverse Address Resolution Protocol. IARP is a protocol that allows a Frame Relay station to discover the protocol address corresponding to a given hardware address. It is more efficient than simulating a broadcast with multiple copies of the same message, and it is more flexible than relying on static configuration. IARP is an extension of the existing ARP, and has the same format as standard ARP.

IARP may be used in any network that provides destination hardware addresses without indicating corresponding protocol.

RARP

Reverse ARP. RARP is a protocol that finds a node's IP address from its DLC address.

SNAP

Subnetwork Access Protocol. SNAP is also called Subnetwork Access Convergence Protocol. An extension to IEEE 802.2 LLC that permits a station to have multiple network-layer protocols. The protocol specifies that DSAP and SSAP addresses must be AA hex. A field subsequent to SSAP identifies one specific protocol. (See RFC 1042 for more detailed information).

TRLR

Trailer format. TRLR is a protocol that is a variant of IP in which the protocol headers follow rather than precede the user data.

SNMP

Simple Network Management Protocol. SNMP is an application-layer protocol for managing TCP/IP based networks. SNMP runs over UDP, which in turn runs over IP. SNMP is organized in terms of network management stations (NMSs), which poll network devices (SNMP agents). At the request of an NMS, an SNMP agent accesses its management information base (MIB) and sends information to the NMS. The MIB provides a standard representation of the SNMP agent's available information and where it is stored.

NOTE: Sniffer Version 5.0 is compatible with SNMP V1 and V2.

CMOT

Common Management and Information Services Protocol (CMIP) over TCP. CMOT is a network management protocol that uses ASN.1 encoding.

SUN Protocol Interpreter Suite

The Sniffer analysis application interprets the protocols that support Sun Microsystems' Network File System (NFS). NFS allows users at workstations to mount directories of files that are located on other machines and to treat them as if they were locally available through the client's operating system. NFS provides an interface that permits a variety of machines (not necessarily under the same operating system) to play the roles of client or server. NFS is composed of a modified UNIX kernel, a set of library routines, and a collection of utilities used by machines that play the role of server.

The Sun PI suite (Figure 2–6) makes use of the session and transport layers of a host network and does not include lower-level protocols of its own. Typically (but not necessarily) Sun NFS runs over TCP/IP on Ethernet. The SUN PI suite interprets frames passed to it by the TCP, IP, or UDP protocols and, thus, requires the TCP/IP PI suite.

Protocols Interpreted

ND

Network Disk. ND is a protocol used to access virtual disks located remotely across the network and to boot diskless workstations.

NFS

Network File System. NFS is a high-level protocol used for communication of requests and responses between network clients and NFS servers. The Sun PI suite interprets NFS Version 3.

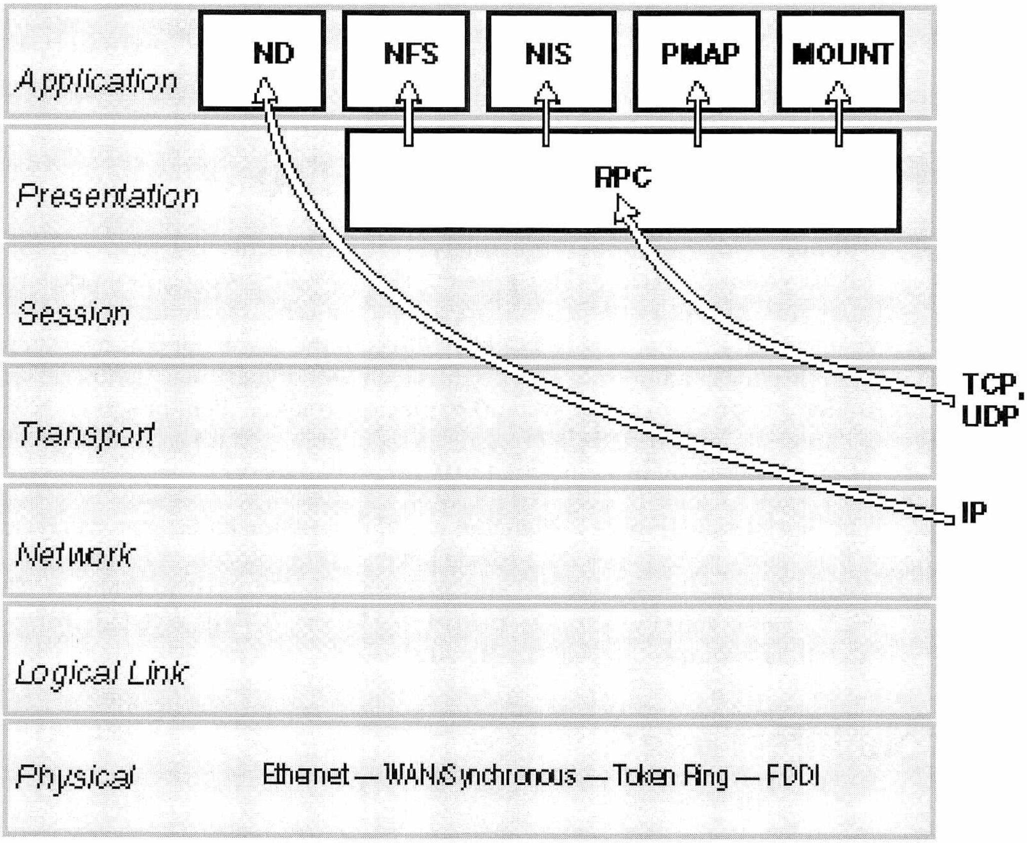


Figure 2–6. The SUN PI Suite Related to the OSI Reference Model

NIS

Network Information Services. NIS is a high-level protocol used for requests and responses regarding the availability of network hosts, services, and directories from a read-only network database.

YP

Yellow Pages. YP is a high-level protocol used for requests and responses regarding the availability of network hosts, services and directories from a read-only network database.

PMAP

Port Mapper. PMAP is a protocol for mapping RPC program numbers to TCP/IP port numbers.

MOUNT

Mount. Mount is a protocol used during initiation of a remote user's access to a network disk, including access checking and account validation.

RPC

Remote Procedure Call. RPC is a protocol for activating a function on a remote station and retrieving the result.

ISO Protocol Interpreter Suite

The Sniffer analysis application interprets the family of protocols built upon recommendations of the International Standards Organization as part of an ongoing international cooperative effort in support of Open Systems Interconnection (OSI). It decodes all layers above the physical layer, which may be any of Ethernet, token ring, or WAN/synchronous. It also decodes Microsoft SMBs. Figure 2–7 shows the ISO protocol interpreter suite.

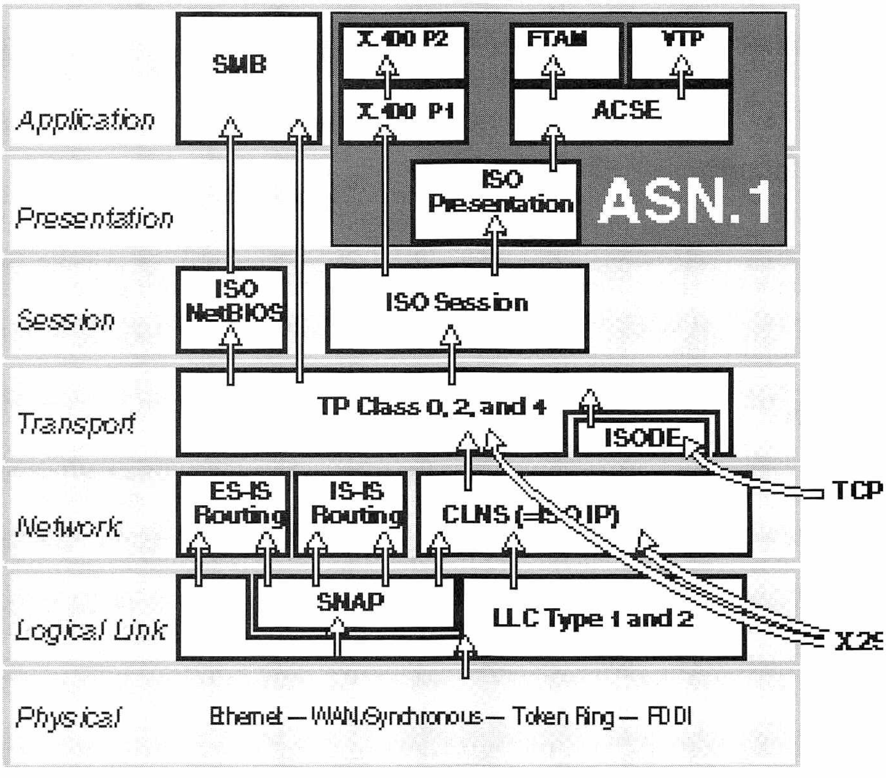


Figure 2–7. The ISO Suite Related to the OSI Reference Model

Protocols Interpreted

X.400

X.400. X.400 is the CCITT 1984 protocol for electronic mail. It consists of two levels: P1 for the addressing of the message's outer envelope and P2 for the inner addressing and content of a personal message.

FTAM

File Transfer and Access Management (ISO 8571/4). FTAM is an OSI protocol that provides access to files stored on dissimilar systems. FTAM is also an international standard.

VTP

Virtual Terminal Protocol (ISO 9041). The Virtual Terminal protocol is an ISO application for establishing a virtual terminal connection across a network.

ACSE

Association Control Service Element (ISO 8650/2). ACSE is an intermediate application-level protocol used in ISO to support a number of more specific application protocols.

Presentation

(ISO 8823). Application data is encoded using the basic encoding rules (ISO 8825) of Abstract Syntax Notation One (ASN.1, ISO 8824). The user may choose to interpret part of these messages either by sharing the generic ASN.1 syntax structure or by displaying the semantics specific to the application-level protocol.

Session

(ISO 8327). The session layer is the fifth layer -- the network processing layer -- in the OSI Reference model. It sets up the conditions whereby individual nodes on the network can communicate or send data to each other. The session layer is responsible for binding and unbinding logical links between users. It manages, maintains, and controls the dialogue between the users of the service. The session layer's many functions include network gateway communications.

SMB

Server Message Block. SMB is a protocol developed by Microsoft for use with the IBM PC LAN Program to make requests from a user station to a server and receive replies. SMB is part of the protocol family that for DOS machines is called MS NET and for OS/2 machines is called the LAN Manager. The OS/2 version of SMB contains extensions not present in the DOS version; both versions are interpreted in the ISO PI suite.

TP

Transport Protocol (ISO 8073). TP is a protocol for which the ISO PI suite interprets class 0 (for connection-oriented networks), class 4 (for connection-less networks) and the intermediate class 2.

CLNS

Connectionless Network Service Protocol (ISO 8473). CLNS is also called ISO IP, for Internetwork Protocol.

ES-IS Routing

End-System to Intermediate-System Routing (ISO 9542). ES-IS is a protocol within the ISO family, used to exchange routing information between gateways and hosts.

IS-IS Routing

Intermediate System to Intermediate System Routing. IS-IS is a protocol within the ISO family, used to exchange routing information between gateways.

LLC

Logical Link Control (ISO 8802/2). LLC is a protocol that provides connection control and multiplexing to subsequent embedded protocols.

TCP/IP Frames

ISODE

ISO Development Environment. ISODE is a protocol used to encapsulate higher-level ISO messages when they are transmitted over a network whose lower levels use TCP/IP. (ISODE serves primarily as a development technique during transition from TCP/IP to ISO protocols).

DECnet Protocol Interpreter Suite

The Sniffer analysis application fully decodes eight protocols defined in Phase IV of Digital Equipment Corporation's *Digital Network Architecture* (DNA). It also decodes several additional protocols that, although not specified in DNA, are used in DECnet systems.

DNA was introduced in 1975 as a master plan for a family of networking hardware and software products valid across a range of machines using both wide-area and local-area networks. Implementation is in phases. Current DEC systems implement Phase V.

DEC provides an implementation of DNA Phase V for each of its operating systems. On LANs, DECnet is commonly used by machines whose physical link is by Ethernet. DECnet protocols can also be used on token ring and WAN/synchronous. The DECnet PI suite can be installed with any of these. Figure 2–8 shows the DECnet protocol interpreter suite.

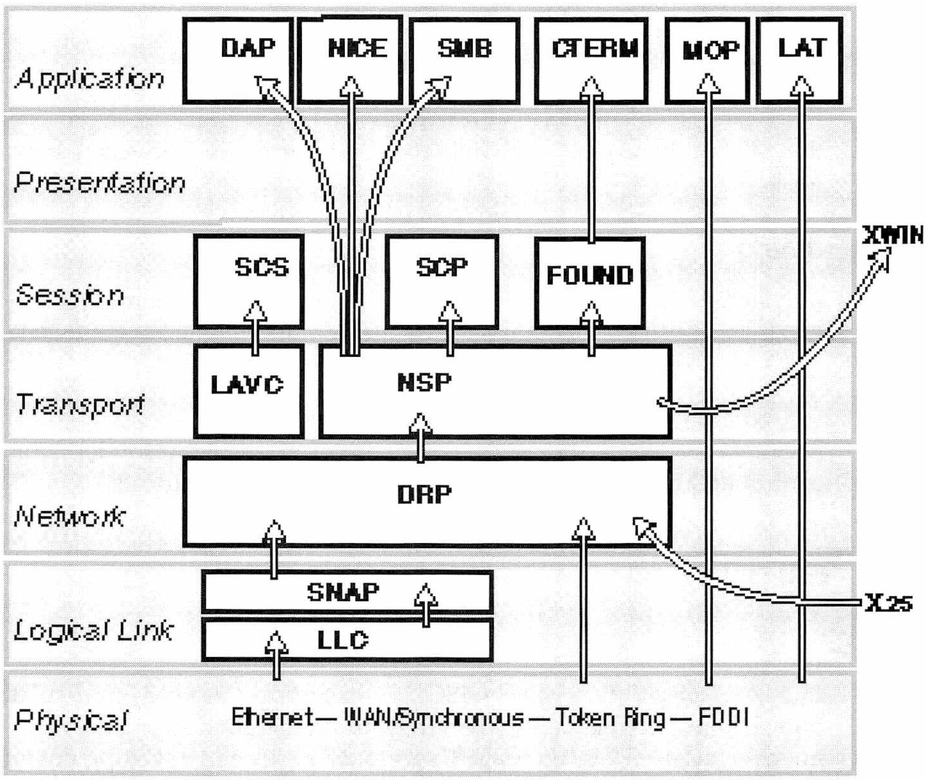


Figure 2–8. The DECnet PI Suite Related to the OSI Reference Model

Protocols Interpreted

DAP

Data Access Protocol. DAP is a protocol that provides remote file access operations. It is a command/response protocol that allows a user process to create new files on a server, open existing files, read and write data, and so on.

LAVC

Local Area VAX Cluster. LAVC is a protocol used to establish and maintain a Local Area VAX Cluster. A cluster is defined as a tightly coupled group of VMS machines. In a tightly coupled group, one computer may depend crucially on another to provide basic services, such as disk access. It is an adaptation of the System Communication Architecture (SCA) that runs over the Ethernet instead of a CI bus.

NICE

Network Information and Control Exchange. NICE is a command/response protocol that provides network management information.

SMB

Server Message Block. SMB is a message type used by the IBM PC LAN Program to make requests from a user station to a server and to receive replies. Many of the functions are similar to those made by an application program to DOS running on a single computer. It is a protocol for remote file access that is very similar in function to DAP and also dwells in the application layer. It was initially developed for the IBM PC LAN Program and is supported by DEC for compatibility.

CTERM

Command Terminal. CTERM is a protocol used for communicating with generic intelligent terminals, i.e., a virtual terminal protocol. It is used in conjunction with FOUND.

FOUND

Foundation Services. FOUND is a protocol used for primitive terminal-handling services and to make and break logical connections between applications and terminals. It is used in conjunction with CTERM.

SCP

Session Control Protocol. SCP is a protocol that establishes virtual circuits based on NSP packets.

NSP

Network Services Protocol. NSP is a protocol that provides reliable message transmission over virtual circuits. Its functions include establishing and destroying logical links, error control, flow control, and segmentation and reassembly of messages.

DRP

DECnet Routing Protocol. DRP is the lowest-level protocol concerned with moving packets from source nodes, through routers, between and within areas, and to end nodes.

MOP

Maintenance Operations Protocol. MOP is a protocol used for network maintenance services that include downline loading, upline dumping, and remote testing and problem diagnosis.

LAT

Local Area Transport Protocol. LAT is a protocol designed to efficiently handle multiplexed terminal (keyboard and screen) traffic to and from timesharing hosts. LAT is a non-DECnet set of protocols that interfaces directly with the LAN and provides an alternative service to CTERM.

LLC

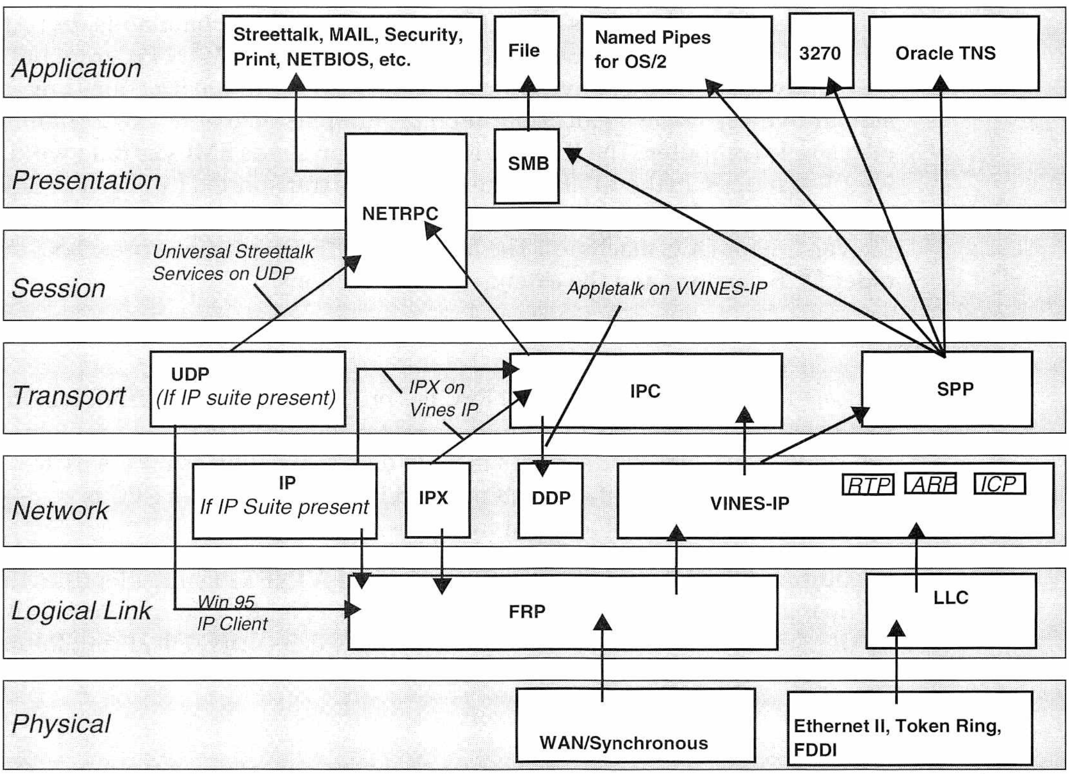
Logical Link Control (IEEE 802.2). LLC is a protocol that provides connection control and multiplexing to subsequent embedded protocols for devices on the token ring.

SNAP

Subnetwork Access Protocol. SNAP is also called Subnetwork Access Convergence Protocol. It is an extension to IEEE 802.2 LLC that permits a station to have multiple network-layer protocols. The protocol specifies that DSAP and SSAP addresses must be AA hex. A field subsequent to SSAP identifies one specific protocol. See RFC 1042 for more detailed information.

Banyan VINES Protocol Interpreter Suite

The Sniffer analysis application interprets protocols in the VINES series developed by Banyan Systems. This release supports Banyan VINES 6.0. VINES links personal computers to file servers on a LAN, perhaps with gateway links to other LANs or WANs. The user stations are PCs, typically running under DOS. Redirection permits directories on the servers to appear to the users as DOS drives, although each server offers these services through processes running on the server's UNIX operating system. The server role may be played by a wide range of devices from different vendors, but all appear to the user in the same way. Figure 2–9 shows the Banyan VINES protocol interpreter suite.



NOTE: Tunnels are only complete if you have all the necessary suites. For example, to decode Appletalk on VINES-IP, you need both Apple and Banyan suites.

Figure 2–9. The Banyan VINES PI Suite Related to the OSI Reference Model

Protocols Interpreted

StreetTalk

StreetTalk. StreetTalk is a protocol used in Banyan VINES to maintain a distributed directory of the names of network resources. Names are global across the internet and independent of the network topology.

MAIL

MAIL. MAIL is a protocol for the transmission of messages in the VINES distributed electronic mail system.

SMB

Server Message Block. SMB is a family of application-layer commands for LAN servers developed by Microsoft for use with the IBM PC LAN Program but frequently used in other environments as well. Many of the functions are similar to those made by an application program to DOS or to OS/2 running on a single computer. The IBM PC LAN Program sends SMBs as data within NetBIOS frames. In the VINES contexts, they are transported by SPP. The SMB protocol for machines running under OS/2 contains extensions not present in the version for DOS machines. The Banyan VINES PI suite interprets both the older DOS versions and the extended OS/2 versions.

Net RPC

Network Remote Procedure Call. Net RPC is a protocol used by the VINES service that provides high-level program-to-program communication and remote procedure calls. Net RPC services include data translation as necessary to match the conventions of sender's and receiver's formats. Net RPC is descended from the protocol that in XNS is called Courier.

In addition to MAIL and StreetTalk, the Banyan VINES PI suite identifies the following protocols that may be transmitted by a Net RPC frame: StreetTalk, MAIL, StreetTalk Directory Assistance, Vanguard Security, File, Print, Route, Echo, and FTP.

IPC

Interprocess Communication Protocol. IPC is a transport-layer protocol providing reliable message service and unreliable datagram service.

SPP

Sequenced Packet Protocol. SPP is a transport-layer protocol providing virtual connection service, based upon the protocol of the same name in XNS.

RTP

Routing Update Protocol. RTP is a protocol used to distribute network topology information. It is used prior to Version 5.5 of Banyan VINES.

SRTP

Sequenced Routing Update Protocol. SRTP is a protocol used to distribute network topology information. It is used in Version 5.5 of Banyan VINES.

ARP

Address Resolution Protocol. ARP is a protocol used for finding a node's DLC addresses from its IP address. It is used prior to version 5.5 of Banyan VINES.

SARP

Sequenced Address Resolution Protocol. SARP is a protocol used for finding a node's DLC addresses from its IP address. Used in version 5.5 of Banyan VINES.

ICP

Internet Control Protocol. ICP is a protocol used to broadcast notification of errors and to note changes in network topology.

VIP

VINES Internet Protocol. VIP is the protocol that moves datagrams throughout the network.

FRP

Fragmentation Protocol. FRP is the protocol that breaks up and reassembles network-layer packets so that they are acceptable to the data-link protocol and the underlying physical medium and to the IP protocol above it.

SNAP

Subnetwork Access Protocol. SNAP is also called Subnetwork Access Convergence Protocol. It is an extension to IEEE 802.2 LLC that permits a station to have multiple network-layer protocols. The protocol specifies that DSAP and SSAP addresses must be AA hex. A field subsequent to SSAP identifies one specific protocol. See RFC 1042 for more detailed information.

LLC

Logical Link Control (IEEE 802.2). LLC is a protocol that provides connection control and multiplexing to subsequent embedded protocols.

AppleTalk Protocol Interpreter Suite

AppleTalk protocols link personal computers (frequently but not necessarily Apple computers) to each other and to external services such as gateways, file servers, or printers. AppleTalk is commonly used over Apple Computer's LocalTalk, Ethernet, or WAN/synchronous or may be encapsulated within packets transmitted by an unrelated protocol, for example TCP/IP.

The Sniffer analysis application interprets frames in both Phase 1 and Phase 2 of the AppleTalk family of protocols. Figure 2–10 shows the AppleTalk protocol interpreter suite.

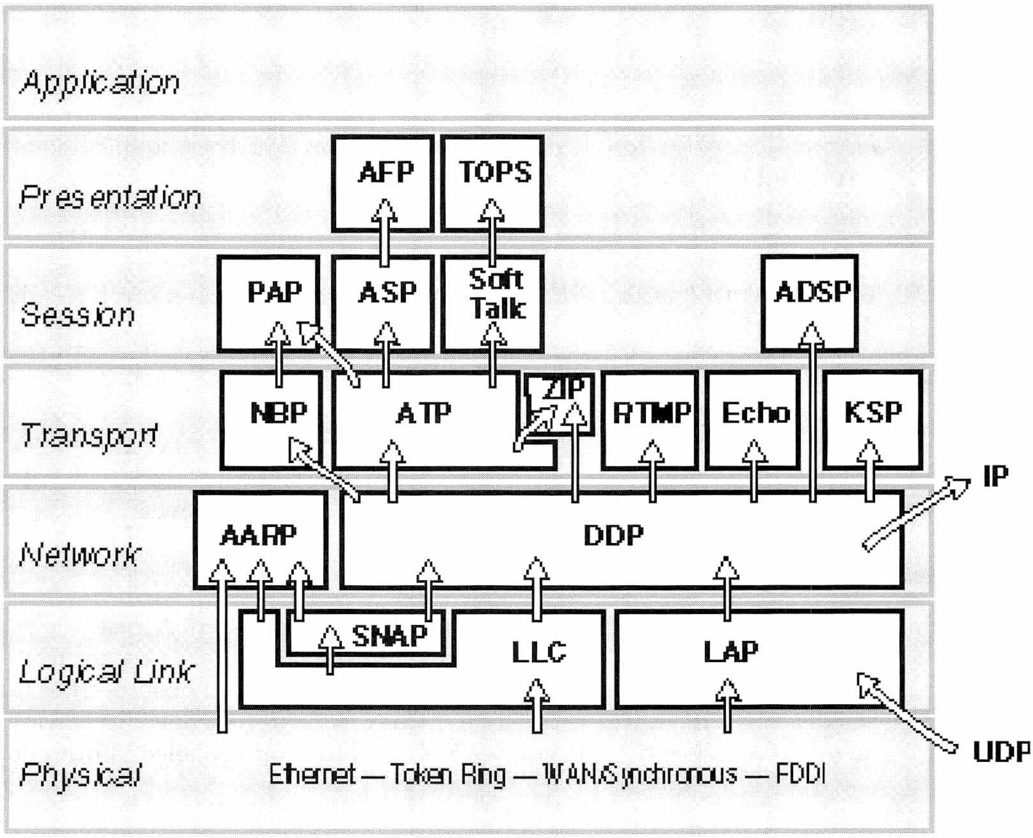


Figure 2–10. The Apple Talk PI Suite Related to the OSI Reference Model

Protocols Interpreted

AFP

AppleTalk Filing Protocol. AFP is a presentation-layer protocol for access to remote files.

TOPS

Transcendental Operating System. TOPS is a presentation-layer protocol used for remote access to files across different operating systems.

SoftTalk

SoftTalk. SoftTalk is a session-layer protocol including support for remote procedure calls used to support TOPS.

PAP

Printer Access Protocol. PAP is a protocol that uses ATP XO ("exactly once") commands to create a stream-like service for communication between user stations and the Apple LaserWriter® or similar stream-based devices.

ASP

AppleTalk Session Protocol. ASP is a general protocol, built upon ATP, providing session establishment, maintenance, and tear-down, along with request sequencing.

ADSP

AppleTalk Data Stream Protocol. ADSP is a connection-oriented protocol providing a reliable, full-duplex, byte-stream service between any two sockets on an AppleTalk internet, ensuring in-sequence, duplicate-free delivery of data over its connections.

NBP

Name-Binding Protocol. NBP is a protocol used in AppleTalk networks to permit network users to refer to network services and sockets by character names. NBP translates a character-string name within a zone into the corresponding socket address.

ATP

AppleTalk Transaction Protocol. ATP is a protocol that provides a loss-free transaction service between sockets, allowing exchanges between two socket clients in which one client requests the other to perform a particular task and report the result.

RTMP

Routing Table Maintenance Protocol. RTMP is a protocol that is used in AppleTalk networks to allow bridges or internet routers to dynamically discover routes to the various subnetworks of an internet. A node that is not a bridge uses a subset of RTMP (the RTMP stub) to determine the number of the network to which it is connected and the node IDs of bridges on its network.

ZIP

Zone Information Protocol. ZIP is a protocol that is used to maintain an internet-wide mapping of networks to zone names for the benefit of routers and as a resource for the name-binding protocol (NBP) to determine which networks belong to a given zone.

Echo

Echo. Echo is a simple protocol that allows any node to send a datagram to any other node and to receive an echoed copy of that packet in return, to verify the node's existence, or to make round trip delay measurements.

KSP

Kiewit Stream Protocol. KSP is a transport protocol resembling TCP developed at Dartmouth College for the support of terminal emulators.

AARP

AppleTalk Address Resolution Protocol. AARP is a protocol that matches the destination address corresponding to a higher-level protocol address.

DDP

Datagram Delivery Protocol. DDP is a protocol that extends the services of the underlying LAP protocol to include an internet of interconnected AppleTalk networks, with provision to address packets to sockets within a node.

SNAP

Subnetwork Access Protocol. SNAP is also called Subnetwork Access Convergence Protocol. It is an extension to IEEE 802.2 LLC that permits a station to have multiple network-layer protocols. The protocol specifies that DSAP and SSAP addresses must be AA hex. A field subsequent to SSAP identifies one specific protocol. (See RFC 1042 for more detailed information).

LLC

Logical Link Control (IEEE 802.2 and ISO/DIS 8802/2). LLC is a protocol that provides connection control and multiplexing to subsequent embedded protocols.

LAP

Link Access Protocol. LAP is the logical-link protocol for AppleTalk. It exists in two variants: ELAP for Ethernet and LLAP for LocalTalk.

X Windows Protocol Interpreter Suite

The Sniffer analysis application interprets the protocol used to transmit information between X Windows clients and servers. The protocol is independent of the lower-level frames that carry its messages. The X Windows PI suite must be installed in combination either with the TCP/IP PI suite where it interprets frames passed to it by TCP, or with the DECnet PI suite where it interprets frames passed to it by NSP. DECWindows is Digital Equipment Corporation's name for X Windows over DECnet.

X Windows is an outgrowth of Project Athena at the Massachusetts Institute of Technology in 1984. Its development was supported by contributions from Digital Equipment Corporation and IBM. Development of the X Windows system is now supported by a consortium that includes the original sponsors and more than 40 additional vendors. The X Windows PI suite interprets the protocol of the consortium's current standard, Version 11, Release 4.

The X system permits a task's graphic display to be treated independently of the task itself. An application's computations may be done anywhere— at any mainframe, minicomputer, or microcomputer that is accessible through the network. The display is handled independently for each user by a *display server.* The rest of the application's work is handled by a process that acts as a remote *client* of the end-user's display server. The client does not need to know anything about the server's hardware or software. It simply describes its output in terms of the X interface. The server must turn that description into a display. The server can maintain contact with several clients at the same time

and, thus, manage multiple windows, sizing, overlaying, moving, or hiding them as the user at the server directs. Figure 2–11 shows the X Windows protocol interpreter suite.

Features of the Interpreter

The X Windows protocol permits a sequence of several commands to be concatenated in a single X message. For transmission, an X message may be fragmented into several frames. The X Windows PI suite reassembles a fragmented message. The hex and detail displays show the entire X message (if captured) starting at the first of its DLC frames. The interpreter's summary window shows a separate line for each X command, regardless of the way the commands may have been packed into lower-level frames.

It may happen that the Sniffer analysis application starts recording after transmission of the initial X Windows setup message. The initial message establishes byte-ordering of the transmitted data, and synchronizes the boundaries of X commands within the transport byte stream. If the interpreter has not seen the initial message, for X messages sent over TCP, the X Windows PI suite uses a heuristic to recognize an X message and to establish the byte-order for its data.

Where a frame includes the selection of options as a sequence of bits, most Sniffer analyzer PIs show all the options, as well as an indication of which were selected. However, some X Windows options are so extensive that listing all of them would require dozens or even hundreds of lines. In such cases, the interpreter shows only the options that are selected and omits those that are not.

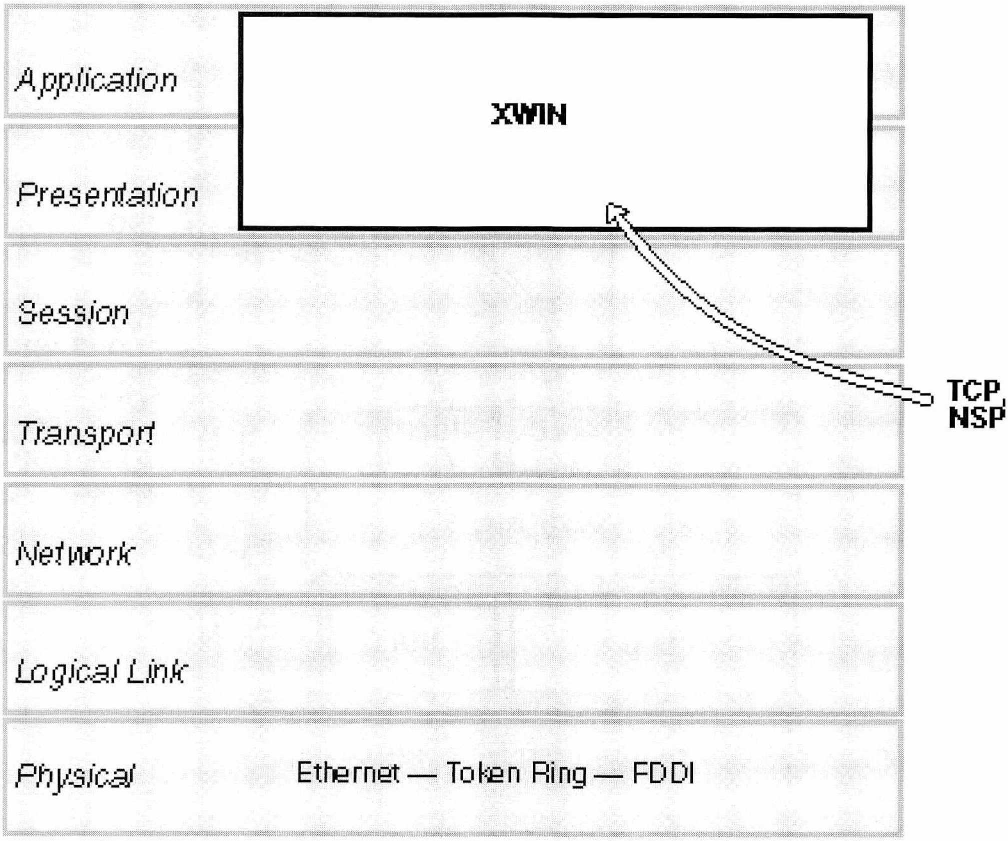


Figure 2–11. The X Windows PI Suite Related to the OSI Reference Model

X.25 Protocol Interpreter Suite

The Sniffer analysis application X.25 PI suite fully decodes six protocols used in the communication links of WANs. It decodes the network Layer 3 of the standard usually known as Recommendation X.25 of the CCITT. Also, it decodes certain protocols commonly used above X.25, identifies several other higher-layer protocols that may be transmitted over X.25, and passes packets to the appropriate PI suites for display. Figure 2–12 shows the X.25 protocol interpreter suite.

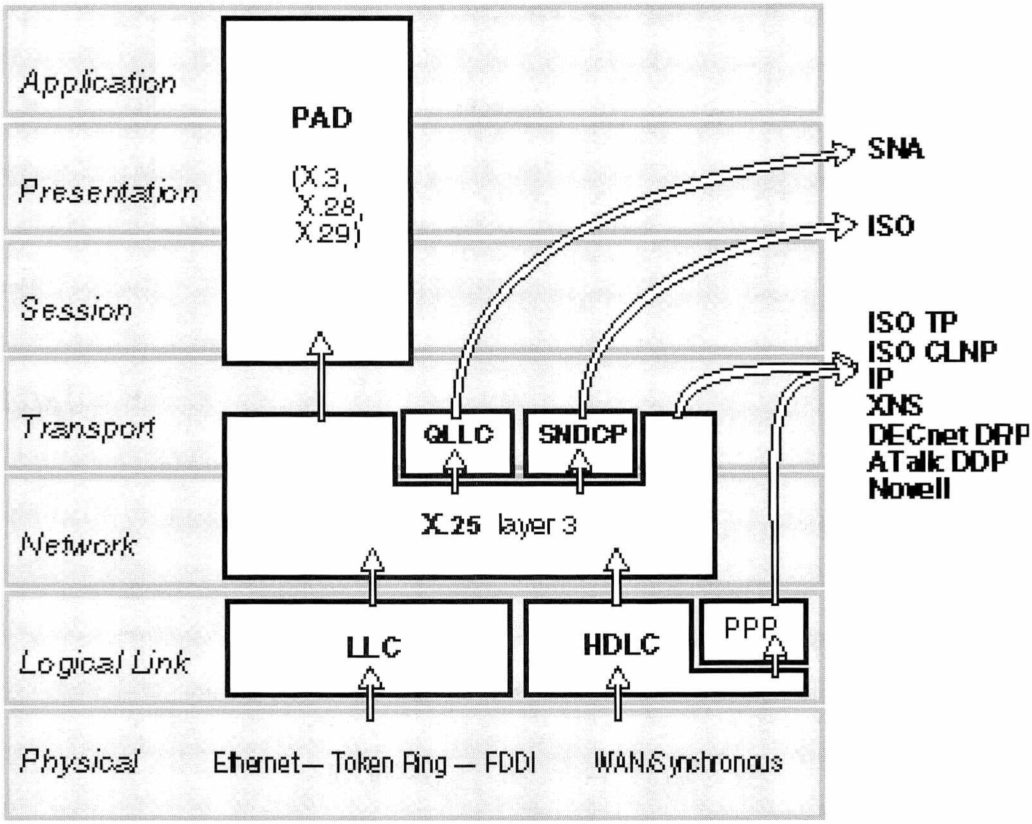


Figure 2–12. The X.25 PI Suite Related to the OSI Reference Model

Protocols Interpreted

PAD

Packet Assembler/Disassembler Protocol. PAD is a protocol family that provides buffering between traffic at a terminal or similar character-oriented device and the block-oriented communications of a packet-switched network. CCITT recommendation X.3 describes a virtual device that acts as an intermediary between the terminal and the X.25 network. The protocol between the terminal and PAD device is described in X.28, and between the PAD device and the X.25 link in recommendation X.29.

X.25

X.25. The Sniffer analysis application X.25 PI decodes Layer 3 of the 1980, 1984 and 1992 versions of CCITT recommendation X.25, including the 1984 extensions for OSI addressing and the ISO and DDN facility and diagnostic fields.

The interpreter recognizes numerous higher-layer embedded protocols and (when installed) passes frames to the appropriate PI suite. Protocols thus interpreted include:

ISO TP and ISO CLNP (with the ISO PI suite); IP (with the TCP/IP PI suite); DRP (with the DECnet PI suite); XNS (with the XNS PI suite); DDP (with the AppleTalk PI suite); and NCP (with the Novell NetWare PI suite).

SNDCP

Subnetwork Dependent Convergence Protocol. SNDCP is an intermediate protocol that provides an interface between X.25 and the transport layer of an ISO protocol. (The enclosed ISO protocols are interpreted when the ISO PI suite is also installed.)

QLLC

Qualified Logical Link Control Protocol. QLLC is an intermediate protocol that provides an interface between X.25 and the SNA family of protocols. (The enclosed SNA protocols are interpreted when the IBM protocol interpreter is also installed in the Sniffer analysis application.)

PPP

Point-to-Point Protocol (RFC 1331). PPP is a link-layer protocol that bypasses X.25 for communication between systems that are directly connected, running any of a variety of protocols directly over HDLC.

HDLC

High-level Data Link Control Protocol. HDLC is the ISO standard protocol that is widely implemented as the logical link layer for an X.25 network. (On IBM networks, the corresponding protocol is called SDLC.) The WAN/Synchronous Sniffer analysis application (Internetwork analyzer) interprets LAPB, the subset of HDLC used to provide link-level support for X.25.

Frame Relay Protocol Interpreter Suite

The Sniffer Internetwork analysis application interprets the Frame Relay protocol. The primary use for Frame Relay is in internetworking — connecting LANs together by means of WAN links. Frame Relay is used to encapsulate the LAN frames so that they can be forwarded properly by the WAN equipment and software.

Frame Relay operates at the network and logical link layers of the OSI reference model. The frame format is optimized for use over networks that have a low rate of physical errors. The number of bytes used for frame overhead is kept as low as possible relative to the number of bytes of LAN data being forwarded. This makes Frame Relay a particularly efficient protocol compared to others in current use.

The logical path from a sending frame relay link through a WAN to a receiving frame relay link is called a virtual circuit. Such a circuit is identified at its source by a Data Link Connection Identifier (DLCI). A network-layer protocol called the Local Management Interface (LMI) is used to keep track of the virtual circuits over which Frame Relay can forward data.

Figure 2–13 shows the relationship among LM1, Frame Relay, and the physical WAN equipment.

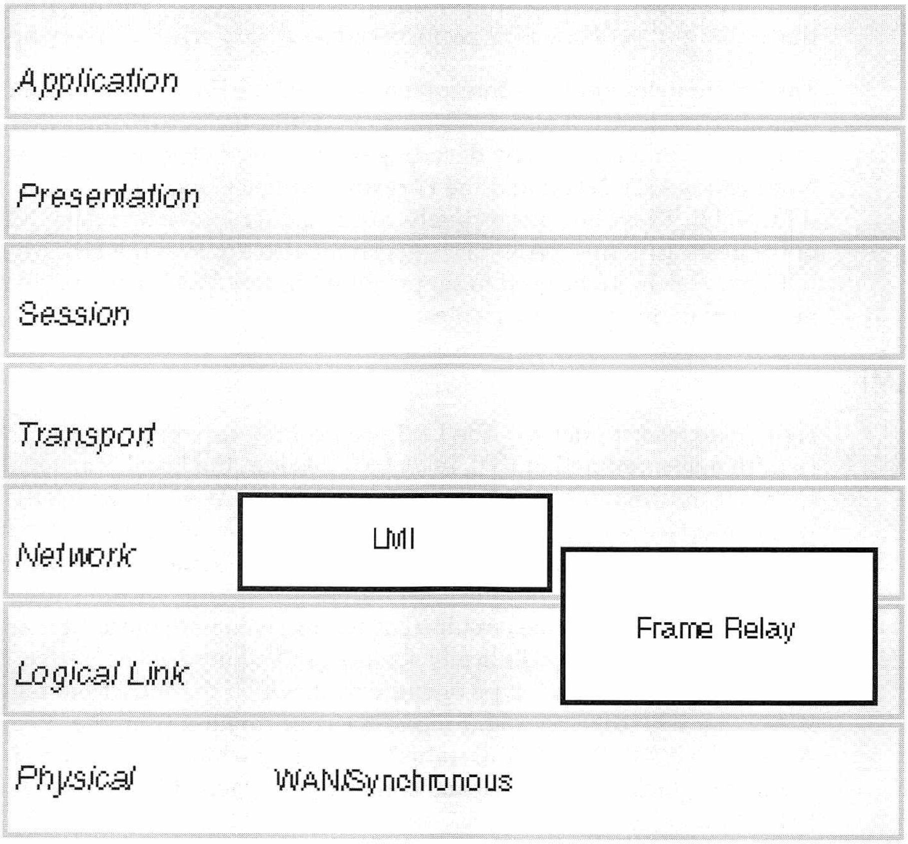


Figure 2–13. The Frame Relay PI Suite Related to the OSI Reference Model

Protocols Interpreted

Frame Relay

The basic frame format for Frame Relay is as follows:

- A one-byte opening flag
- A short header (typically two bytes, containing ten DLCI address bits and six control bits)
- User (subscriber) data (a variable length field)
- A two-byte frame check sequence
- A one-byte closing flag

If a frame is defective in any way, or if WAN congestion precludes its delivery, the Frame Relay protocol simply discards the frame. It is the responsibility of the higher protocol layers to perform the necessary error recovery operations.

The Frame Relay protocol interpreter decodes the Frame Relay header and identifies the DLCI. It also determines from this header whether there is any congestion on the WAN, by decoding the Backward Explicit Congestion Notification (BECN) bit and the Forward Explicit Congestion Notification (FECN) bit. These bits, respectively, notify a data source or a data destination of congestion on the WAN. The interpreter also decodes the Discard Eligible (DE) bit, which can be used to set priorities, in case WAN congestion makes it necessary to discard some frames.

LMI

Local Management Interface. The LMI protocol interpreter complies with the requirements outlined in RFC 1490. LMI decodes the Local Management Interface information, which is maintained by the WAN to which the Frame Relay interface is attached. The LMI frames are special Frame Relay frames, identified by DLCI = 1023. The LMI information is contained in the user data area of the Frame Relay frame. LMI frames are used to inform subscribers of the status of all the virtual circuits that are involved with the local Frame Relay link. Each subscriber periodically sends a Status Enquiry LMI frame. This can be a simple "keep alive" type of enquiry, in which the subscriber tells the WAN that it is still active, and receives a confirmation from the WAN. Alternatively, it can be a "full status" request, to which the WAN responds by giving the status of all the virtual connections attached to the local Frame Relay link.

SMT Protocol Interpreter Suite

The Sniffer analysis application interprets the SMT protocol, which is used to manage stations on an FDDI network. SMT contains these components:

- Connection management (CMT) connects nodes to the FDDI network, manages physical connection between adjacent PHYs, configures PHY and MAC entities within a node, and coordinates trace functions.
- Ring management (RMT) receives status information from MAC and CMT and reports this status to SMT and higher-level processes.
- SMT frame services provide the means to control and observe the FDDI network.

Figure 2–14 shows the relationship between SMT, MAC, and LLC. The FDDI standards deal specifically with MAC, SMT, and the physical aspects of FDDI.

Although Logical Link Control (LLC) is not part of the FDDI standards, FDDI requires LLC for proper operation and data transmission.

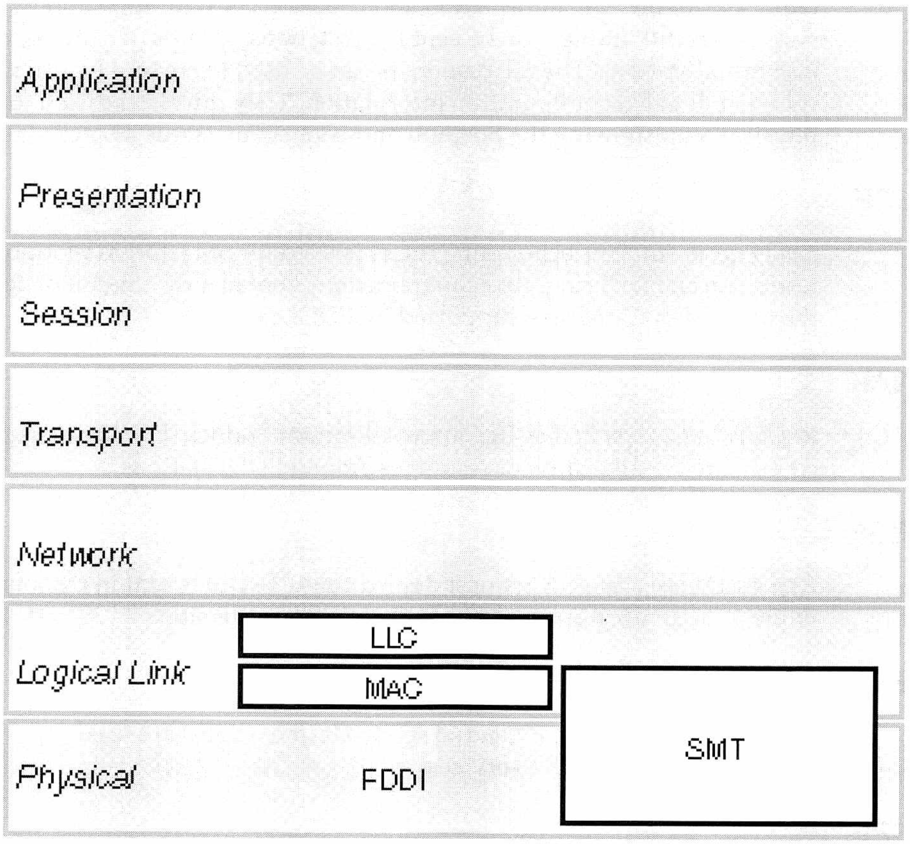


Figure 2–14. The SMT PI Suite Related to the OSI Reference Model

Features of the Interpreter

The SMT protocol interpreter decodes the following SMT frames:

NIF

Neighbor Information Frame. Each station sends out neighbor information frames (NIFs) to its downstream neighbor at intervals of 30 seconds or less. This keeps each station informed as to the address of its upstream neighbor. In addition, a monitoring station can use these frames to construct a logical ring map showing the order in which the stations on the ring appear in the token path.

SIF

Status Information Frame. A station can use a status information frame (SIF) to request or to provide information about station configuration and operating parameters. SIF frames can be sent to all stations, groups of stations, or to individual stations. The SIF responses can be used to create a logical ring map showing detailed configuration information. They can also be used to create a physical map showing the position and connection status of each station.

ECF

Echo Frame. An SMT echo frame (ECF) is used for SMT-to-SMT loopback testing on an FDDI ring. An echo frame may contain any amount of data up to the maximum frame size supported by FDDI.

RAF

Resource Allocation Frame. Resource Allocation Frames (RAFs) are used to coordinate the allocation of resources among FDDI stations.

RDF

Request Denied Frame. A request denied frame (RDF) is sent in response to a request for an unsupported frame class, type, or version.

ESF

Extended Service Frame. Extended service frames (ESFs) are used for extending and exercising new SMT services.

SRF

Status Report Frame. Status report frame (SRFs) are used to periodically announce station status that may be of interest to the manager of an FDDI ring.

PMF

Parameter Management Frame. Parameter management frames (PMFs) are used for remote management of station attributes.

Oracle SQL*Net V2 Protocol Interpreter

The Sniffer analysis application interprets the Oracle SQL*Net V2, which is the primary protocol used to connect Oracle7 servers and clients. In this documentation, SQL*Net V2 refers to the Transparent Network Substrate (TNS) and the SQL*Net layer. SQL*Net V2 provides client-to-server and server-to-server communication between Oracle applications and databases. It offers a protocol-independent interface from higher-layer SQL applications to lower-layer, connection-oriented transport protocols such as TCP/IP, SPX, NetBios, DECnet, AppleTalk and others.

The TNS is a session-layer protocol that provides the following services:

- Establishes connection to servers and MultiProtocol Interchange
- Sends commands and data packets
- Establishes session parameters such as what security and data integrity options.

The SQL*Net is the presentation/application-layer protocol that provides the following services:

- Establishes logon to the database
- Sets Oracle7 protocols and client-server data types
- Sends SQL commands
- Receives server responses or client data * Orderly logout from the database

Client to server sessions are established using the TNS Connect and Accept packet types. The TNS Redirect and Resend are used to specify the servers to which the Connect request should be sent.

Once the session is established, practically all communications between the application and the database is done through the TNS Data packet. The data packet has the logon request and response, data types and protocols, and the SQL query and responses. These commands and responses may consist of one or more TNS data packets. A TNS data packet may consist of one or more frames depending on the transport-layer protocol used.

Figure 2–15 shows the SQL*Net V2 protocol in the context of the OSI model along with sample higher layer applications.

Sniffer 5.0 decodes only the frames with valid TNS headers. It does not reassemble fragmented frames. It does, however, identify data packets that are made of multiple frames. Later revisions of the product will do the message reassembly.

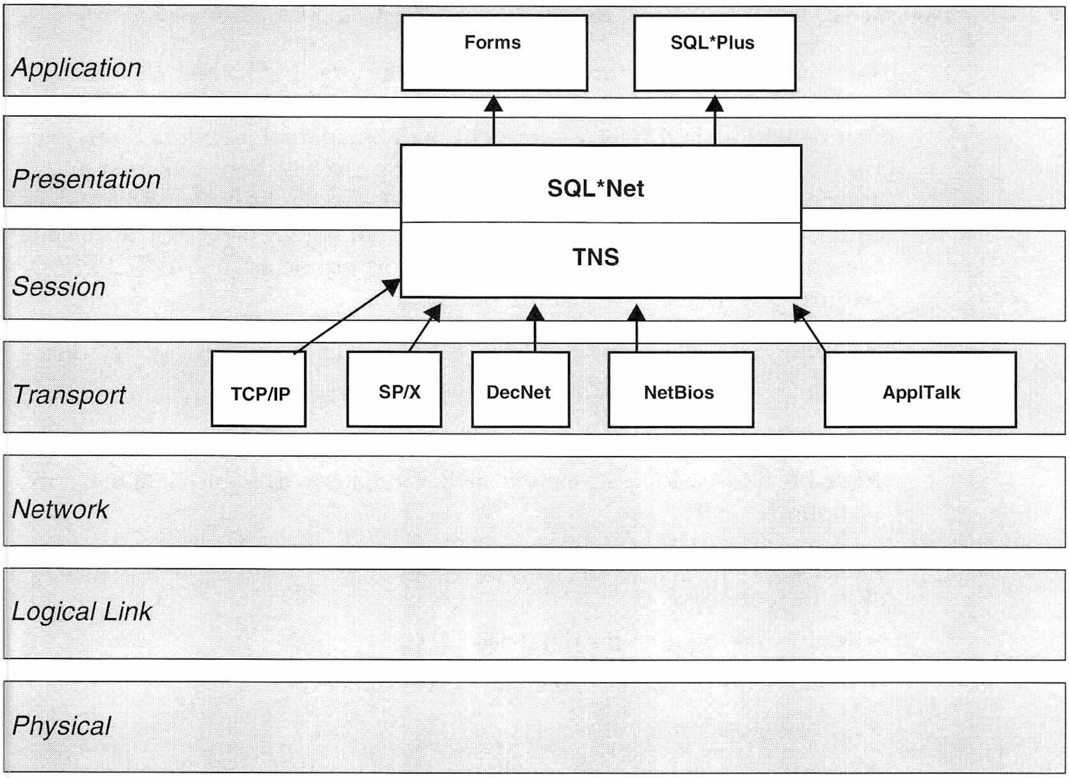


*Figure 2–15. Oracle SQL*Net V2 in the OSI Model*

Sybase TDS Protocol Interpreter

The Sniffer analysis application interprets the Sybase TDS (Tabular Data Stream) protocol. Sybase TDS creates a common interface from higher-layer SQL applications to lower-layer, connection-oriented transport protocols, such as TCP/IP, SPX, NetBios, DECnet, and others. In effect, TDS makes the lower layers "transparent" to the SQL programmer, allowing the coding of higher-layer applications without reference to the underlying protocols.

Sybase TDS performs the following services:

- Establishes connections to servers
- Requests data and server status
- Receives data, status, error information, and other server results
- Requests stored procedures

- Provides orderly shut down for connections

Sybase TDS is mostly a token-based protocol where:

- A token is a single-byte value that indicates the format and/or value of the data to follow. This self-describing format allows clients to request data without knowing in advance such details as field types, number of values returned, and other information stored in the server.
- A token describes fixed or variable-length data.
- Fixed-length tokens don't have a length field.

NOTE: Data streams used for client login and bulk transfer of data do not use tokens.

Figure 2–16 shows the Sybase TDS protocol in the context of the OSI model, along with some sample higher-layer applications.

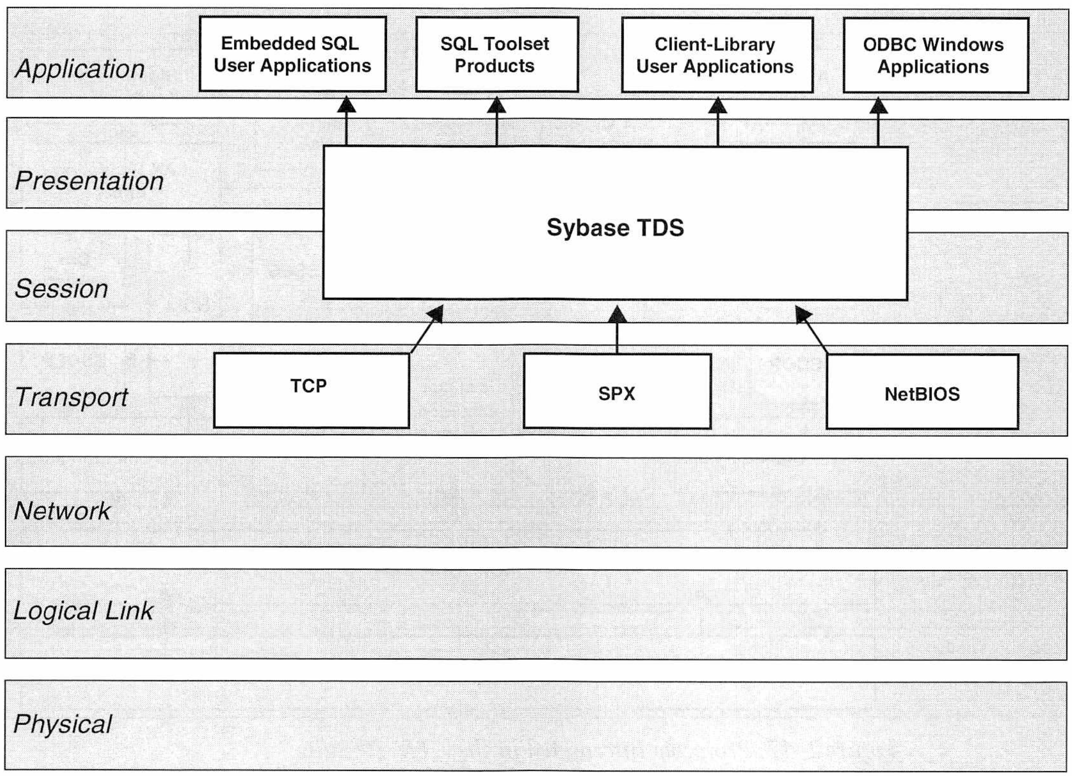


Figure 2–16. Sybase TDS in the OSI Model

ATM Protocol Interpreter Suite

The Sniffer analysis application fully decodes protocols used in ATM networks. It decodes Layer 3 (the ATM adaptation layer) of the B-ISDN standard protocol stack found in Recommendation I.321 of the ITU-T. Also, it decodes certain protocols commonly used above ATM (such as LAN Emulation), identifies several other higher-layer protocols that may be transmitted over ATM (such as IP), and passes packets to the appropriate PI suites for display. Table 2–17 shows the ATM protocol interpreter suite.

The ATM Sniffer analysis application can also capture and decode raw cells (that is, Layer 2 of the B-ISDN protocol stack found in ITU-T Recommendation I.321). You specify whether the analyzer should capture raw cells or should reassemble cells into higher layer frames using the **Reassemble frames** option in the analysis application's main menu. See the *Analyzer Operations* manual for details.

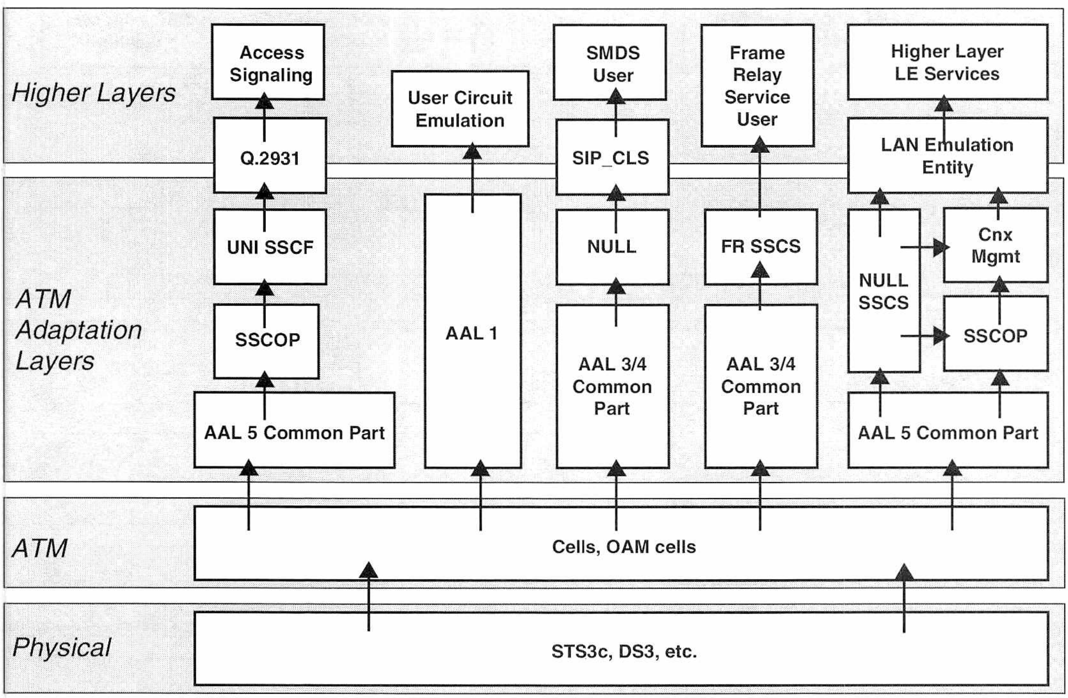


Figure 2–17. Protocols Interpreted in the ATM PI Suite

Protocols Interpreted

Q.2931

The Sniffer analysis application decodes Signaling AAL as defined in the ITU-T Recommendation Q.2931 (previously known as Q.93B). Q.2931 provides the signaling function in the B-ISDN protocol stack. It is used for point-to-point connection setup and release, VPI/VCI selection and assignment, Quality of Service class requests, basic error handling, and specification of Peak Cell Rate (PCR) traffic parameters, among other functions.

SSCF

Service Specific Coordination Function. The Sniffer analysis application decodes SSCF as defined in ITU-T Recommendation Q.2130. Along with SSCOP, SSCF is part of the protocol model for Signaling AAL (SAAL) and is found at the AAL layer of the B-ISDN protocol model. It performs (among other services) the following functions:

- Assured data transfer mode
- Unacknowledged data transfer mode
- Independence from the underlying layers
- Transparent relay of information
- Establishment of connections for assured data transfer mode

SSCOP

Service Specific Connection-Oriented Protocol. The Sniffer analysis application decodes SSCOP as defined in ITU-T Recommendation Q.2110. SSCOP is a peer-to-peer protocol found at the AAL layer of the B-ISDN protocol model. It is part of the protocol model for SAAL. It performs (among other services) the following functions:

- Guaranteed ordered delivery
- Error correction
- Receiver-based flow control
- Error reporting to layer management
- Ability to set up, tear down, and synchronize an SSCOP connection

OAM

Operations, Administration, and Management. The Sniffer analysis application decodes the OAM cells found at the physical and ATM layers in the B-ISDN protocol stack. OAM cells are used for performance management, fault management, and other administrative tasks. There are various defined OAM cell types indicated by a reserved value in a cell's header. OAM cell types include Alarm Indication Signal, Remote Defect Indication, and Far End Receive Failure, among others.

LAN Emulation

LAN Emulation is a set of services that allows a legacy LAN to be emulated over ATM. In a LAN Emulation environment, there are several entities, including the LAN Emulation Client (LEC), the LAN Emulation Server (LES), the Broadcast and Unknown Server (BUS), and the LAN Emulation Configuration Server (LECS). Each of these entities communicates with one another using defined protocols, such as the Initialization protocol, the Registration protocol, and so on. The Sniffer analysis application decodes the various protocols associated with LAN Emulation services.

ILMI

Interim Local Management Interface. The Sniffer analysis application decodes ILMI. ILMI is an SNMP-based management protocol for an ATM UNI defined by the ATM Forum. It is found over either the AAL 3/4 or the AAL 5 layer.

Appendix A
Glossary of Terms

1BASE5 The implementation of the IEEE 802.3 standard using 1 Mbps transmission on a baseband medium whose maximum segment length is 500 meters.

10BASE2 The implementation of the IEEE 802.3 (Ethernet) standard using 10 Mbps transmission on a baseband medium whose maximum segment length is 185 meters.

10BASE5 The implementation of the IEEE 802.3 (Ethernet) standard using 10 Mbps transmission on a baseband medium whose maximum segment length is 500 meters.

10BASE-T The implementation of the IEEE 802.3 (Ethernet) standard using 10 Mbps transmission on a baseband medium. The standard provides a means for attaching AUI-compatible devices to 24 gauge, unshielded twisted-pair cable, instead of the usual coaxial media.

100BASE-Tx The implementation of the IEEE 802.3 (Ethernet) standard using 100 Mbps transmission on a baseband medium. The standard provides a means for attaching AUI-compatible devices to 24 gauge, unshielded twisted-pair cable, instead of the usual coaxial media.

3Com 3+ A networking system from 3Com Corporation using parts of the XNS and Microsoft/IBM PC LAN program protocols.

3Plus 3Com's implementation of XNS. Interpreted by the XNS PI suite.

802.2 The IEEE standards designation for the LLC sublayer protocol that provides both datagram and reliable connection transmission.

802.3 The IEEE standards designation for the CSMA/CD network access method. Similar to (and often used interchangeably with) Ethernet.

802.4 The IEEE standards designation for token bus networks. Used primarily with MAP protocols.

802.5 The IEEE standards designation for the token ring network access method.

AARP AppleTalk Address Resolution Protocol. For outgoing packets, supplies the hardware destination address corresponding to a higher-layer protocol address, and filters incoming packets to pass only those that are broadcast or specifically addressed to it. Interpreted in the AppleTalk PI suite.

AC Access Control. A DLC byte on IEEE 802.5 token ring networks that contains the token indicator and frame priority information.

ACK Acknowledge. A network packet acknowledging the receipt of data.

ACSE Association Control Service Element. An ISO application-layer protocol interpreted in the ISO PI suite.

ACT Absolute Congestion Threshold. A Frame Relay term.

active monitor A computer on a token ring that acts as the controller for the ring, regulating the token and other performance aspects.

ACTPU Activate Physical Unit. An SNA message sent to start a session.

ADSP AppleTalk Data Stream Protocol. A connection-oriented protocol providing a reliable, full-duplex, byte-stream service between any two sockets on an AppleTalk internet. Interpreted in the AppleTalk PI suite.

advertising The process by which a service makes its presence known on the network. Typically provided through a LAN-based multicast.

AEP AppleTalk Echo Protocol. *See* **Echo**.

AFP AppleTalk Filing Protocol. A presentation-layer protocol for access to remote files. Interpreted in the AppleTalk PI suite.

AIS Alarm Indication Signal (T1 lines). A T1 alarm signal consisting of any string of 2048 ones containing fewer than three zeros.

ALAP AppleTalk Link Access Protocol. *See* **LAP**.

alarm Network statistics sent from a DSS Server to a connected Console over a LAN or WAN. Triggered by the monitor or analyzer application on the Server when network statistics exceed certain thresholds. Consists of the name of an offender, a timestamp, and an alarm priority threshold.

alert Notification of an alarm condition. Sent from a Distributed Sniffer System Server to a non-connected unit such as a pager or a Console. Consists of a numeric identifier and a numeric value of the alarm threshold.

AMI Alternate Mark Inversion (T1 Lines). A pulse transmission T1 line coding scheme that uses alternating polarities in the pulse train.

ANSI American National Standards Institute. An industry-supported organization dedicated to the development of trade and communication standards; internationally, the American representative to the International Organization for Standardization.

API Application Program Interface. The specification of functions and data used by one program module to access another; the programming interface that corresponds to the boundary between protocol layers.

APPC Advanced Program-to-Program Communications. A communications system used to communicate between transaction programs on IBM computers; APPC uses the LU 6.2 subset of SNA.

APPN Advanced Peer-to-Peer Networking. APPN is second-generation Systems Network Architecture (SNA). APPN extends SNA to environments without mainframes, where midrange processors need to communicate as peers.

architecture The architecture of a system refers to how the system is designed and how the components of the system are connected to, and operate with, each other.

ARCNET

A baseband token-passing network originally designed by the Datapoint Corporation that communicates among up to 255 stations at 2.5 Mbps.

ARP

Address Resolution Protocol. A protocol within TCP/IP for finding a node's DLC address from its IP address. Interpreted in the TCP/IP PI suite. Also interpreted in the Banyan VINES PI suite.

NOTE: After VINES version 5.5 this protocol is identified within VINES as SARP.

ASCII

American Standard Code for Information Interchange. A mapping between numeric codes and graphical characters used almost universally for all personal computer and non-IBM mainframe applications.

ASN.1

Abstract Syntax Notation One. A set of conventions governing the ISO presentation layer. Interpreted in the ISO PI suite.

ASP

AppleTalk Session Protocol. A general protocol built upon ATP providing session establishment, maintenance, and tear-down, along with request sequencing. Interpreted in the AppleTalk PI suite.

asynchronous transmission

A method of data transmission which allows characters to be sent at irregular intervals by preceding each character with a start bit and following it with a stop bit. Commonly used to communicate with modems and printers.

ATM

Asynchronous Transfer Mode (Cell relay). A standard that defines a set of network services for transmitting data for high-speed LANs or WANs. The basic packet is a fixed-length cell of 53 octets (bytes), 5 of which are used for control functions and 48 for data.

ATP

AppleTalk Transaction Protocol. Provides a loss-free transaction service between sockets, allowing exchanges between two socket clients in which one client requests the other to perform a particular task and report the result. Interpreted in the AppleTalk PI suite.

AUI

Attachment Unit Interface. Drop cable for Ethernet between station and transceiver.

backbone — The backbone is the part of the communications network which carries the heaviest traffic. It is one basis for design of the overall network service.

background service — A protocol transmitted by a Net RPC frame in Banyan VINES.

background task — A secondary job performed while the user is performing a primary task. For example, many network servers will carry out the duties of the network (controlling communications) in the background while, at the same time, the users are running their own applications (such as word processors) in the foreground.

bandwidth — The amount of data that can be moved through a particular communications link. For example, Ethernet has a bandwidth of 10 Mbps.

baseband — A transmission technique that sends data bits without using a much higher carrier frequency (contrast with broadband). The entire bandwidth of the transmission medium is used by one signal.

baud rate — A measure of signaling speed in data communications. Specifies the number of signal elements that can be transmitted each second. For most purposes, at slow speeds, a baud rate is the same as the speed in bits per second.

BCC — Block Check Character. Another word for Frame Check Sequence (FCS).

beacon — A token ring packet that signals a serious failure on the ring.

BECN — Backward Explicit Congestion Notification (Frame Relay). The sixth bit in the second octet of the frame relay header. Used to inform a subscriber device of congestion in the backward direction.

BER — Bit Error Rate. The percentage of received bits in error compared to the total number of bits received. Usually expressed exponentially.

BERT — Bit Error Rate Test. Test used to ascertain the bit error rate on a given wide-area link.

BGP	Border Gateway Protocol. BGP, as defined in RFC 1771, allows the user to create loop-free interdomain routing between autonomous systems.
BIND	An SNA message sent to activate a session between logical units.
BIOS	Basic Input/Output System. A set of routines that work closely with the hardware to support the transfer of information between elements of the system such as memory, disks, and the monitor.
bipolar	The predominant signaling method used for digital transmission services, such as DDS and T1.
BIS	Bracket Initiation Stopped. An SNA message sent to indicate that the sending station will not attempt to initiate any more brackets.
BLER	Block Error Rate. The rate of occurrence of blocks with errors, calculated as the ratio of erroneous blocks received over total blocks.
BLERT	Block Error Rate Test. A device that calculates and reports the block error rate for a communication system.
BNC	Bayonet-Neill-Concelman. A standardized coaxial cable connector; used for Thin Ethernet ("Cheapernet") cables and ARCNET networks.
BOOTP	Boot Protocol. A protocol within TCP/IP that is used for downloading initial programs into networked stations. Interpreted in the TCP/IP PI suite.
BPV	Bipolar Violation (T1 lines). A violation of the alternating pulse rule, caused by a single detection error in a bipolar signaling system.
breakout box	A test device used to view the signals in an RS-232, V.35, or other interface. The breakout box is used to diagnose problems with the interface.
bridge	A device used to connect two separate networks into one extended network. Bridges only forward packets between networks that are destined for the other network.

broadband — A transmission technique that sends data bits encoded within a much higher radio-frequency carrier signal. The transmission medium may be shared by many simultaneous signals since each one only uses part of the available bandwidth.

broadcast — (1) A message directed to all stations on a network or collection of networks.

(2) A destination address that designates all stations.

buffer — A software program, storage space in RAM, or a separate device used to store data. For example, the Sniffer Network Analyzer's capture buffer serves as a temporary storage space for captured network data until it can be analyzed or saved to disk.

bursty traffic — Data communications term referring to an uneven pattern of data transmission.

capture — The process in which the Sniffer analysis application records network traffic for interpretation. Generally speaking, this interpretation takes place during **display**. However, the Expert Sniffer analysis application can simultaneously capture and interpret network traffic.

CCITT — Consultative Committee for International Telegraphy and Telephony. CCITT is a member of the International Telecommunications Union (ITU) that is, in turn, a specialized body within the United Nations. It sponsors a number of standards dealing with data communications networks, telephone switching standards, digital systems, and terminals.

CGA — Color Graphics Adapter. The interface between a personal computer and a medium-resolution color monitor.

chat script — A group of three chat strings (Setup, Listen, and Disconnect) that control communication parameters for an asynchronous device.

chat string — A UNIX-style command/response sequence of characters which are downloaded to a serial device in order to control the device.

CIR Committed Information Rate. The largest number of bits per second that a frame relay network agrees to carry for a PVC. CIR is assigned at the time of subscription to the frame relay service.

client (1) A module that uses the services of another module. The session layer is a client of the transport layer, for example.

(2) A PC or workstation that accesses services or applications from another "server" PC or workstation.

CLLM Consolidated Link Layer Management. An access signaling protocol specified by ANSI for Frame Relay links.

CLNS Connectionless Network Service Protocol (also called ISO IP). Interpreted in the ISO PI suite.

CMIP Common Management Information and Services Protocol. When used with TCP/IP, it is also known as CMOT.

CMOT Common Management Information and Services Protocol Over TCP. A management protocol for networks; it uses ASN.1 encoding. Interpreted in the TCP/IP and ISO PIs.

compression Reducing the bandwidth or bits necessary to encode information.

concentrator A central point for connecting many individual stations to a network ring. Found most often on FDDI networks.

Courier A presentation-layer protocol in XNS (similar to RPC in the Sun protocol family); it delivers data to such application-layer protocols as XNS Printing, XNS Filing, or XNS Clearinghouse.

CRC Cyclic Redundancy Check. A check-word, typically two or four bytes at the end of a frame, used to detect errors in the data portion of the frame.

CSMA/CA Carrier Sense Multiple Access with Collision Avoidance. A random access or contention-based control technique; the algorithm used in LocalTalk networks to control transmission.

CSMA/CD Carrier Sense Multiple Access with Collision Detection. A random access or contention-based control technique; the algorithm used by IEEE 802.3 and Ethernet networks to control transmission.

CSU	Channel Service Unit. An interface to a common carrier's transmission facilities that ensures that digital signals placed on the line are properly shaped and timed. It usually is combined with a data service unit (DSU).
CSV	Comma Separated Values. A common file format used for importing data into spreadsheet programs.
CTERM	Command Terminal. A protocol within DECnet for communicating with generic intelligent terminals, that is, a virtual terminal protocol. Interpreted in the DECnet PI suite.
CTS	Clear to Send. A signal used in serial communications; sent, as from a modem to its computer, to indicate that transmission can proceed. CTS is a hardware signal sent over line 5 in RS-232-C connections.
DAC	Dual Attachment Concentrator. A concentrator that offers two connections to the FDDI network capable of accommodating the FDDI dual ring, and additional ports for connection of other concentrators or FDDI stations.
DAP	Data Access Protocol. The DECnet protocol that provides remote file access. Interpreted in the DECnet PI suite.
DAS	Dual Attachment Station. An FDDI station that offers two connections to the FDDI dual counter-rotating ring.
DB-9	A 9-pin standardized connector used in personal computers for a token ring network connection (female), serial I/O port (male), and RGBI output. Also used for LocalTalk.
DB-15	A 15-pin standardized connector used at the transceiver, the drop cable, and the station of IEEE 802.3 or Ethernet network components.
DB-25	A 25-pin standardized connector used in personal computers for parallel output ports (female connector on IBM PC chassis) or for serial I/O ports (male connector on IBM PC chassis).
DCE	Data Circuit-terminating Equipment (also called Data Communications Equipment). On a serial communications link, the device that connects the DTEs into the communication line or channel.

DDP

Datagram Delivery Protocol. Extends the services of the underlying link access protocol to include an internet of interconnected AppleTalk networks, with provision to address packets to sockets within a node. Interpreted in the AppleTalk PI suite.

DDS

Dataphone Digital Service. An AT&T leased service that provides digital communications channels to subscribers at a wide range of bit rates.

DE

Discard Eligibility. The seventh bit of the second octet of the frame relay header. A value of 1 in the DE bit indicates that the frame is eligible for discard by a congested network.

destination address

That part of a message which indicates for whom the message is intended.

DFC

Data Flow Control. An SNA subprocess for reliable message transfer.

diagnosis

A problem on the network detected by the Expert Sniffer analyzer. The Expert Sniffer analyzer detects and alerts users to diagnoses as it discovers them on the network to which it is attached.

DIP switch

Dual In-Line Package switch. A small switch usually attached to a printed circuit board. Usually requires a small screwdriver to change. There are only two settings– on or off. Printed circuit boards usually have "banks" of multiple DIP switches used to configure the board in a semi-permanent way.

DIS

Draft International Standard. One of the stages in defining ISO protocols. Final stage is IS.

DISC

Disconnect. An LLC non-data frame indicating that the connection established by an earlier SABM or SABME is to be broken.

display

The process in which the Sniffer analyzer interprets the traffic recorded during capture. During display, the analyzer decodes the various layers of protocol in the recorded frames and displays them as English abbreviations or summaries.

DIX DEC/Intel/Xerox. Used to refer to an early version of Ethernet.

DLC Data Link Control. The lowest protocol layer within the transmitted network frame; fields typically include the destination address, the source address, and perhaps other control information.

DLCI Data Link Connection Identifier. A 10-bit number used by the Frame Relay protocol to identify a virtual circuit.

DLL (1) Downline load. A protocol within the Datapoint RMS family used for downloading initial programs into networked stations.

(2) Dynamic Link Library. A type of program library used in MS-Windows.

DM Disconnected Mode. An LLC message acknowledging that a previously established connection has been broken.

DNS Domain Name Service. A protocol within TCP/IP for finding out information about resources using a database distributed among different name servers. Interpreted in the TCP/IP PI suite.

DRP DECnet Routing Protocol. The lowest-layer DECnet protocol, concerned with moving packets from endnodes through routers to other endnodes.

DS0 Digital Signal level 0 (T1 lines). A single 64 Kbps channel in a DS1 signal. *See also* **DS1**.

DS1 Digital Signal level 1 (T1 lines). The basic digital signal for transmission over T1 facilities. The DS1 signal consists of 24 channels at 64 Kbps (called DS0, or Digital Signal level 0, channels), plus 8 Kbps used for synchronization and signaling, for a total bandwidth of 1,544 Kbps.

DSAP Destination Service Access Point. The LLC SAP for the protocol expected to be used by the destination station in decoding the frame data.

DSS

Distributed Sniffer System. Network General's client-server network analysis solution. A Distributed Sniffer System consists of Sniffmaster Consoles controlling network monitoring and analysis tools known as Sniffer Servers. With a DSS, network managers can diagnose the problems of a complex, geographically dispersed network from a centralized location.

DSU

Data Service Unit. A device that connects terminal equipment to digital communications lines. *See also* **CSU**.

DTE

Data Terminal Equipment. On a serial communications link, a generic term used to describe the host or end-user machine.

duplex

A characteristic of data transmission. Either full or half duplex. Full permits simultaneous two-way communication. Half means only one side can talk at a time.

DVMRP

Distance Vector Multicast Routing Protocol. DVMRP is a protocol for routing multicast datagrams through an internet.

E1

A digital transmission link with a capacity of 2.048 Mbps (CCITT version of T1).

EBCDIC

Extended Binary Coded Decimal Interchange Code. A mapping between numeric codes and graphical characters used for IBM mainframe computers and communications protocols defined by IBM.

Echo

(1) A request/response protocol within XNS used to verify the existence of a host.

(2) A protocol within AppleTalk that allows any node to send a datagram to any other node and to receive an echoed copy of that packet in return to verify the existence of that node or to make round-trip delay measurements. Interpreted in the AppleTalk PI suite.

(3) A protocol transmitted by a Net RPC frame in Banyan VINES.

ECF — Echo Frame. ECF is a protocol in which an SMT echo frame (ECF) is used for SMT-to-SMT loopback testing on an FDDI ring. An echo frame may contain any amount of data up to the maximum frame size supported by FDDI.

EGP — Exterior Gateway Protocol. A protocol within TCP/IP used to exchange routing information among gateways belonging to the same or different systems. A generalization of gateway-to-gateway protocol.

EIA — Electronic Industries Association. A standard organization specializing in the electrical and functional characteristics of interface equipment.

EIGRP — Extended Interior Gateway Routing Protocol. EIGRP is an enhanced version of IGRP. It is a suite of Cisco routing protocols used in TCP/IP and OSI internets.

ELAP — *See* LAP.

Error — A protocol within XNS by which a station reports that it has received (and is discarding) a defective packet. Interpreted in the XNS PI suite.

error rate — In data transmission, the ratio of the number of incorrect elements transmitted to the total number of elements transmitted.

ESF — Extended Superframe Format (T1). A modification of the DS1 format that uses the 193rd bit to signal line problems.

ESIA — Expert Sniffer Internetwork Analyzer. Network General's internetwork analyzer with Expert that analyzes and interprets internetworking problems in real time. It interprets 140 encapsulated LAN protocols over leased line, frame relay, or X.25 circuits.

ES-IS Routing — End-System to Intermediate-System Routing. A protocol within the ISO family used to exchange routing information between gateways and hosts. Interpreted in the ISO PI suite.

ESNA — Expert Sniffer Network Analyzer. Network General's stand-alone diagnostic tool that observes the local or wide area network to which it is attached, translates bit streams into plain English, and interprets monitored activity in real time.

Ethernet A CSMA/CD network standard originally developed by Xerox; similar to (and often used interchangeably with) the IEEE 802.3 standard.

Ethertype A 2-byte protocol-type code in Ethernet frames used by several manufacturers but independent of the IEEE 802.3 standard.

FC Frame Control. On a token ring network, the DLC byte that contains the frame's type.

FCS *See* **Frame Check Sequence**.

FDDI Fiber Distributed Data Interface. An ANSI/ISO standard that defines a 100 Mbps LAN over a fiber-optic medium using a timed token over a dual ring of trees.

FE Framing Error. An error that occurs due to incorrect framing of data units transmitted. In asynchronous transmission, this is usually due to a deviation in the stop bit cell.

FECN Forward Explicit Congestion Notification (Frame Relay). The fifth bit in the second octet of the frame relay header. Used to inform a subscriber device of congestion in the forward direction.

FEP Front-End Processor. The "traffic cop" of the data communications world. Typically sits in front of a computer and is designed to handle the telecommunications burden so the computer can concentrate on handling the processing burden.

FID Format Identification. A field in the systems network architecture (SNA) transmission header indicating the type of nodes participating in the conversation. For example, LU 6.2 nodes are type 2.

filter The Sniffer analysis application uses several varieties of filters, including the following:

(1) **Capture filters**. These filters determine which arriving frames the analyzer discards and which it retains.

(2) Display filters. These filters determine which frames in the capture buffer will be displayed. Eliminating a frame from display with a display filter does not remove the frame from memory.

flow control — Hardware or software mechanisms used in data communications to turn off transmission when the receiving workstation is unable to store the data it is receiving. Various methods of regulating the flow of data during a conversation. Buffers are an example of flow control.

FMD — Function Management Data. A class of data embedded at the start of systems network architecture (SNA) request unit/response units.

FMH — Function Management Header. The header part of SNA FMD containing addressing and transmission control information.

FOUND — Foundation Services. A protocol within DECnet used for primitive terminal-handling services. Interpreted in the DECnet PI suite.

frame — The multibyte unit of data transmitted at one time by a station on the network; synonymous with "packet."

frame check sequence (FCS) — In bit-oriented protocols, a 16-bit field added to the end of a frame that contains transmission error-checking information.

Frame Relay — A streamlined access protocol commonly used for LAN interconnectivity.

FRMR — Frame Reject. An LLC command or response indicating that a previous frame had a bad format and is being rejected. The FRMR frame contains five bytes of data explaining why and how the previous frame was bad.

Front-End Processor — *See* **FEP**.

FRP — Fragmentation Protocol. Breaks up and reassembles network-layer packets so that they are acceptable to the data-link protocol and the underlying physical medium; used on networks whose physical medium is ARCNET. Interpreted in the Banyan VINES PI suites.

FS

Frame Status. A byte appended to a token ring network frame following the CRC. It contains the Address Recognized and Frame Copied bits.

FTAM

File Transfer, Access and Management. An application-layer protocol within the ISO suite, on top of ACSE.

FTP

File Transfer Protocol.

(1) A protocol based on TCP/IP for reliable file transfer. Interpreted in the TCP/IP PI suite.

(2) A protocol transmitted by a Net RPC frame in Banyan VINES.

functional address

A limited broadcast destination address for IEEE 802.5 token ring networks. Individual bits in the address specify attributes that stations eligible to receive the frame should have. Similar to "multicast address."

gateway

In the general sense, a gateway is a computer that connects two different networks together. Usually, this means two different kinds of networks, such as SNA and DECnet. In TCP/IP terminology, however, a gateway connects two separately administered subnetworks, which may or may not be running the same networking protocols.

GGP

Gateway-to-gateway protocol. A protocol within TCP/IP used to exchange routing information between IP gateways and hosts. Interpreted in the TCP/IP PI suite. *See also* **EGP**.

Gopher

Gopher is an Internet protocol designed for distributed document search and retrieval. It acts as a document delivery system. The protocol and software follow a client-server model on a TCP connection.

GUI

Graphical User Interface, pronounced "gooey." An operating system or environment that displays options on the screen as icons, or picture symbols.

handshaking

The electrical exchange of predetermined signals when a connection is made between two devices carrying data. Just as people shake hands when they meet, computers must go through a procedure of "greeting" the opposite party and preparing for communications.

HDLC High-level Data Link Control. A standard bit-oriented protocol developed by the International Standards Organization (ISO). In HDLC, control information is always placed in the same position. Specific bit patterns used for control differ dramatically from those used to represent data, minimizing errors. Many internetworking companies (such as Cisco and Vitalink) have developed proprietary versions of HDLC which the Sniffer Internetwork analysis application can decode.

header The beginning portion of a message which contains destination address, source address, message-numbering, and other information. The header helps direct the message along its journey. Different protocols implement headers in different ways.

heartbeat On Ethernet, the SQE signal generated by the transceiver at the end of a transmitted frame to check the SQE circuitry. *See* **SQE TEST**.

hop A term used in routing. A hop is one data link. A path to the final destination on a net is a series of hops away from the origin. Each hop has a cost associated with it, allowing the calculation of a least cost path.

hub A concentrator and repeater for the network. Generally speaking, a hub is a central point for wiring or computing in a network.

IARP Inverse Address Resolution Protocol. IARP allows a Frame Relay station to discover the protocol address corresponding to a given hardware address.

ICMP Internet Control Message Protocol. A protocol within TCP/IP used principally to report errors in datagram transmission. Interpreted in the TCP/IP PI suite.

ICP Internet Control Protocol. Used to broadcast notification of errors and to note changes in network topology in Banyan VINES. Interpreted in the XNS PI suite.

ID Identification.

IDP Internet Datagram Protocol. Delivers to an internet address a single frame as an independent entity, without regard to other packets or to the addressee's response.

IEEE Institute of Electrical and Electronics Engineers, Inc. Standards documents are available from them at 345 East 47th Street, New York, NY 10017.

I-Frame Information Frame. An LLC, HDLC, or SDLC frame type used to send sequenced data that must be acknowledged.

IGMP Internet Group Management Protocol. IGMP is used to keep neighboring multicast routers informed of the host group memberships present on a particular local network.

IGRP Interior Gateway Routing Protocol. Cisco routing protocol designed for campus-wide use, as opposed to wide-area use.

I/O Input/Output. The part of a computer system or the activity that is primarily dedicated to the passing of information into or out of the central processing unit or memory.

IONET Input/Output Network. A device message protocol used by Datapoint.

IP Internet Protocol. The lowest-layer protocol under TCP/IP that is responsible for end-to-end forwarding and long packet fragmentation control. Interpreted in the TCP/IP PI suite. A similar protocol is interpreted in the Banyan VINES PI. *See also* **IPX** and **ISO IP**.

IPC Interprocess Communication Protocol. A transport-layer protocol in Banyan VINES, providing reliable message service and unreliable datagram service. Interpreted in the Banyan VINES PI suite.

IPX Internet Packet Exchange. Novell's implementation of Xerox Internet Datagram Protocol. Interpreted in the Novell NetWare PI suite.

IS (1) International Standard. The final phase for an ISO protocol definition. At this point, the protocol is fully specified and guaranteed not to change.

(2) Intermediate System. An OSI term for a system that originates and terminates traffic, and that also forwards traffic to other systems.

ISDN

Integrated Services Digital Network. A digital telephone technology that combines voice and data services on a single circuit. Source of many ideas for frame relay networking.

IS-IS Routing

Intermediate System to Intermediate System Routing. IS-IS is a protocol within the ISO family, used to exchange routing information between gateways.

ISO

International Organization for Standardization (or International Standards Organization).

(1) A consortium that is establishing a suite of networking protocols.

(2) The protocols standardized by that group.

ISODE

ISO Development Environment. Protocol for transmitting higher-layer ISO protocols over a network whose lower layers are handled by TCP/IP. Interpreted in the TCP/IP and ISO PI suites.

ISO IP

The ISO standard Internet Protocol. Interpreted in the ISO PI suite.

KSP

Kiewit Stream Protocol. A transport protocol resembling TCP developed at Dartmouth College for the support of terminal emulators connected to AppleTalk networks; interpreted in the AppleTalk PI suite.

LAN

Local Area Network. The hardware and software used to connect computers together in a limited geographical area.

LAP

Link Access Protocol. The logical-layer protocol for AppleTalk. It exists in two variants: ELAP (for Ethernet) and LLAP (for LocalTalk networks). Interpreted in the AppleTalk PI.

LAPB

Link Access Protocol Balanced. A subset of HDLC.

LAPD

Link Access Protocol-D. A link control protocol based on HDLC that is related to ISDN.

LAST

Local Area System Transport. Protocol for remote booting in DECnet/DOS.

LAT — Local Area Transport. The DECnet protocol that handles multiplexed terminal (keyboard and screen) traffic to and from timesharing hosts. Interpreted in the DECnet PI suite.

LATA — Local Access and Transport Area. The geographic area in which a local exchange telephone carrier is permitted to operate.

LAVC — Local Area Vax Cluster. An adaptation of the System Communication Architecture (SCA) to run over the Ethernet instead of a CI bus. Used to enable MicroVAXs to operate as diskless nodes.

leased line — Same as a leased circuit, dedicated circuit, or leased channel. A telephone line rented for exclusive continuous use. Commonly used to connect LANs remote from one another.

link protocol — The set of rules by which a logical data link is set up and by which data transfers across the link. Includes formatting of the data.

LLAP — *See* **LAP**.

LLC — Logical Link Control. A protocol that provides connection control and multiplexing to subsequent embedded protocols; standardized as IEEE 802.2 and ISO/DIS 8802/2.

LMI — Local Management Interface. An access signaling protocol defined for Frame Relay circuits. LMI carries information on the status of permanent virtual circuits between the network and a subscriber device. Optional additions to LMI include multicasting, global addressing, and flow control.

LOOP — Loopback. A protocol under Ethernet for sending diagnostic probe messages.

LSA — Lost Subarea. An SNA error condition.

LSB — Least Significant Bit. The lowest-order (usually rightmost) bit of a binary number.

LSD — Least Significant Digit. The lowest-order, or rightmost, digit in the normal representation of a number.

LU 6.2 — Logical Unit 6.2. A subset of the SNA protocols used for peer-to-peer communications between computers.

LUSTAT Logical Unit Status. An SNA message used to send status information.

MAC Medium Access Control. The protocol layer that describes network management frames sent on the 802.5 token ring. Most MAC frames are handled transparently by the network adapter.

Mail Service Protocol used (in conjunction with StreetTalk) for the transmission of messages in the VINES distributed electronic mail system. Interpreted in the Banyan VINES PI suite.

Manchester encoding A data encoding technique that uses a transition at the middle of each bit period that serves as a clock and also as data.

MAP Manufacturing Automation Protocol. A multilayer networking protocol developed primarily by General Motors for manufacturing control applications.

Matchmaker Obsolete term for Net RPC.

MAU Multiple Access Unit (also known as a Medium Attachment Unit). The wiring concentrator or transceiver used for attaching stations connected to the network.

MIB Management Information Base. The structured database of network statistical information used by the SNMP and CMIP protocols.

MIC Media Interface Connector. An optical fiber connector pair that links the fiber media to the FDDI node or another cable.

modem A contraction of modulate and demodulate; a conversion device installed in pairs at each end of an analog communications line. The modulator part of the modem codes digital information onto an analog signal by varying the frequency of the carrier signal. The demodulator part extracts digital information from a modulated carrier signal.

MOP Maintenance Operations Protocol. A protocol under DECnet for remote testing and problem diagnosis. Interpreted in the DECnet PI suite.

MOUNT A protocol developed by Sun Microsystems that provides request access checking and user validation. It is used in conjunction with NFS. Interpreted in the Sun PI suite.

MSB Most Significant Bit. The highest-order bit of a binary number, not including the sign bit.

multicast (1) A message directed to a group of stations on a network or collection of networks (contrast with broadcast).

(2) A destination address that designates such a subset.

multiplexing Sending several signals over a single line and separating them at the other end.

NAK Negative Acknowledgment. A response from the recipient of data to the sender of that data to indicate that the transmission was unsuccessful (that is, that the data was corrupted by transmission errors).

NBP (1) Name-Binding Protocol. Used in AppleTalk networks to permit network users to use character names for network services and sockets. NBP translates a character-string name within a zone into the corresponding socket address. Interpreted in the AppleTalk PI suite.

(2) NetBIOS Protocol. Used in 3Com 3+ Open software. Interpreted in the XNS PI suite.

NC Network Control. An SNA subprocess.

NCP NetWare Core Protocol. Novell's application-layer protocol for the exchange of commands and data between file servers and workstations. Interpreted in the Novell NetWare PI suite.

ND Network Disk. A protocol within the Sun NFS family used to access virtual disks located remotely across the network. Interpreted in the TCP/IP PI suite.

NDS Netware Directory Services Protocol. NDS is a Novell protocol that operates with NCP to manage IPX routing.

NetBIOS Network Basic Input/Output System.

(1) A protocol implemented by the PC LAN Program to support symbolically named stations and the exchange of arbitrary data.

(2) The programming interface (API) used to send and receive NetBIOS messages.

There are several different and incompatible implementations of NetBIOS, and separate PIs for them, as, for example, in the IBM and the TCP/IP PI suites.

NETBLT

Network Block Transfer. A protocol within earlier versions of TCP/IP. Not interpreted in the TCP/IP PI suite.

Net RPC

Protocol used by the VINES service that provides high-level program-to-program communication, including translation as necessary to match the conventions of sender's and receiver's formats. Net RPC is descended from XNS Courier. Interpreted in the Banyan VINES PI suite.

NetWare

The networking system designed by Novell Inc. and the protocols used therein.

network object

The Expert Sniffer analysis application creates network objects by performing multilayer protocol analysis on the frames that pass through its real-time protocol interpreters. In this way, the Expert analyzer can distill a relatively small number of network objects from the huge body of information it processes. Network objects can be any of the following: a DLC station, a network station, a connection, an application, or a subnetwork.

network topology

The geography of a network. Examples of network topologies include ring, bus, and star.

NFS

Network File System. A protocol developed by Sun Microsystems for requests and responses to a networked file server. Interpreted in the Sun PI suite.

NGCP

Network General Control Protocol. Network General Corporation protocol used for communications between Distributed Sniffer System consoles and servers.

NIC

Network Interface Card. A circuit card that implements the DLC layer connection of a station to a network.

NICE Network Information and Control Exchange. The DECnet protocol for network management. Interpreted in the DECnet PI suite.

NIF Neighbor Information Frame. Used by stations on an FDDI ring to announce their addresses to downstream neighbors.

NIS Network Information Services. Previously known as "Yellow Pages." A set of services in the Network File System (NFS) that propagate information from masters to recipients. Used for the maintenance of system files on complex networks.

NLSP Netware Link Services Protocol. NLSP is a link-state protocol that improves the performance, reliability, scalability, and manageability of IPX traffic in large-scale LAN-WAN internetworks.

NNTP Network News Transfer Protocol. NNTP is a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the ARPA-Internet community.

nodes Points on a network where service is provided, service is used, or communications channels are interconnected. "Node" is sometimes used interchangeably with "workstation."

N(R) Receive sequence number. An LLC or HDLC field for Information frames that indicates the sequence number of the next frame expected; all frames before N(R) are thus implicitly acknowledged.

NRZ Non-return to Zero. A way of encoding binary signals that aims to achieve the highest possible data transfer rate for a given signal frequency.

NRZI Non-return to Zero Inverted. A binary encoding scheme that inverts the signal on a "one" and leaves the signal unchanged for a "zero." The Sniffer Internetwork analysis application can interpret both NRZ and NRZI, but you must set the correct option in the **Options** menu.

N(S) Send sequence number. An LLC or HDLC field for Information frames that indicates the sequence number of the current frame within the connection.

NSP	Network Services Protocol. The DECnet protocol that provides reliable message transmission over virtual circuits. Interpreted in the DECnet PI suite.
NTP/SNTP	Network Time Protocol/Simple Network Time Protocol. NTP or SNTP provides the mechanisms to synchronize time and coordinate time distribution in a large, diverse internet.
null modem	A cross-pinned cable used for DTE to DTE communications. Sometimes called a modem eliminator.
octet	A string of eight bits. Synonymous with Byte.
OpenNET	A networking system from the Intel Corporation that uses parts of the OSI standards and components of the Microsoft/IBM PC LAN program. Interpreted in the ISO PI suite.
OSI	Open Systems Interconnection. A generalized model of a layered architecture for the interconnection of systems.
overhead	Work or information that provides support for a computing process but is not an intrinsic part of the operation or data. In communications, for example, error checking is a form of overhead that is added to messages so that sending and receiving programs can verify transmission.
packet	The multibyte unit of data transmitted at one time by a station on the network. Synonymous with "frame."
packet switching	A method for sending data in packets through a network to some remote location. The data to be sent is subdivided into individual packets of data, each having a unique identification and carrying its destination address. This way, each packet can go by a different route, possibly arriving in a different order than it was shipped. The packet ID allows the data to be reassembled in proper sequence.
PAD	Packet Assembler Disassembler. Special purpose computer on an X.25 network that allows asynchronous terminals to use the synchronous X.25 network by packaging asynchronous traffic into packets.

PAP
Printer Access Protocol. A protocol within AppleTalk that uses ATP XO commands to create a stream-like service for communication between user stations and the Apple LaserWriter or similar stream-based devices. Interpreted in the AppleTalk PI suite.

parallel interface
An interface which permits parallel transmission, or simultaneous transmission of the bits making up a character or byte, either over separate channels or on different carrier frequencies of the same channel.

parity bit
A binary bit appended to an array of bits to make the sum of the bits always odd or always even. Used with a parity check for detecting errors in transmitted binary data.

parity check
A process for detecting whether bits of data have been altered during transmission of that data.

patch panel
A device in which temporary connections can be made between incoming and outgoing lines. Used for modifying or reconfiguring a communications system or for connecting test instruments (such as the Sniffer Network Analyzer) to specific lines.

PCF
Physical Control Fields. The part of the token ring DLC header that includes the AC and FC fields.

PC*I
Personal Computer Integration. Data General's nomenclature for their networking system. Protocols used include the ISO IP and TP4 levels and the Microsoft/IBM PC LAN program SMB protocols. Interpreted in the ISO PI suite.

PDU
Protocol Data Unit. The data delivered as a single unit between peer processes on different computers.

PEP
Packet Exchange Protocol. A protocol within the XNS family used to exchange datagrams. Interpreted in the XNS/MS-Net PI suite.

PI
Protocol Interpreter. A program that knows the frame format and transaction rules of a communications protocol and can decode and display frame data.

PING
A TCP/IP tool supplied with TCP/IP Distributed Sniffer System. PING is a diagnostic utility that sends ICMP Echo Request messages to a specific IP address on the network.

PMAP

Port Mapper. A protocol developed by Sun Microsystems for mapping RPC program numbers to TCP/IP port numbers. Interpreted in the Sun PI suite.

PMF

Parameter Management Frame. Parameter management frames (PMFs) are used for remote management of station attributes.

POP3

Post Office Protocol - Version 3. POP3 permits a workstation to dynamically access a mail facility on a server host.

port

The physical access point to a computer, multiplexer, device, or network where signals may be sent or received.

PPP

Point-to-Point Protocol (RFC 1331). PPP is a link-level protocol that bypasses X.25 for communication between systems that are directly connected, running any of a variety of protocols directly over HDLC.

preamble

A fixed data pattern transmitted before each frame to allow receiver synchronization and recognition of the start of a frame.

Presentation

The presentation layer is the sixth layer of the OSI model (ISO 8823). It controls the formats of screens and files. Control codes, special graphics, and character sets work in this layer.

protocol

A specific set of rules, procedures, or conventions governing the format and timing of data transmission between two devices.

protocol interpreter

The Sniffer analysis application uses its protocol interpreters to identify the protocols nested within each frame and interpret their contents.

PUP

PARC Universal Packet. A type of Ethernet packet formerly used at the Xerox Corporation's Palo Alto Research Center. Interpreted in the XNS/MS-Net and the TCP/IP PIs but not included in their protocol diagrams since no longer in regular use.

PVC

Permanent Virtual Circuit. A unique, predefined logical path between two endpoints of a network. Used by Frame Relay.

QLLC Qualified Logical Link Control Protocol. QLLC is an intermediate protocol that provides an interface between X.25 and the SNA family of protocols. (The enclosed SNA protocols are interpreted when the IBM protocol interpreter is also installed in the Sniffer analysis application.)

RAF Resource Allocation Frame. Resource allocation frames (RAFs) are used to coordinate the allocation of resources among FDDI stations.

RARP Reverse Address Resolution Protocol. A protocol within TCP/IP for finding a node's IP address given its DLC address. Interpreted in the TCP/IP PI suite.

RDF Request Denied Frame. A request denied frame (RDF) is sent in response to a request for an unsupported frame class, type, or version.

RDP Reliable datagram protocol. A protocol within an earlier version of TCP/IP. Not interpreted in the TCP/IP PI suite.

REJ Reject. An LLC frame type that requests retransmission of previously sent frames.

REM Ring Error Monitor. A station on the 802.5 token ring network that collects MAC-layer error messages from the other stations.

repeater A device inserted at intervals along a circuit to boost, amplify, and/or regenerate the signal being transmitted.

RFC Request For Comment. Designation used in DoD/TCP protocol research and development.

RG-58 The designation for 50-ohm coaxial cables used by Cheapernet (thin Ethernet).

RG-59 The designation for 75-ohm coaxial cables used by PC Network (broadband).

RG-62 The designation for 93-ohm coaxial cables used by ARCNET.

RGBI Red-Green-Blue-Intensity. An interface used for attaching a color monitor to a personal computer; DB-9 connectors are typically used.

RH

Request/Response Header. An SNA control field prior to a Request Unit or Response Unit.

RI

Routing Information. A protocol at the logical link layer for devices operating on the token ring. Interpreted by the token ring or Ethernet Sniffer analysis application independent of other PIs.

RII

Routing Information Indicator. If the first bit in the source address field of a token ring frame is 1, then the data field begins with Routing Information. Interpreted by the token ring or Ethernet Sniffer analysis application independent of other PIs.

RIP

Routing Information Protocol. A protocol within the XNS and TCP/IP families used to exchange routing information among gateways. Interpreted in the XNS PI suite and in the TCP/IP PI suite.

RISC

Reduced Instruction Set Computer. A type of microprocessor design that focuses on rapid and efficient processing of a relatively small set of instructions.

RJ-45

The designation for the 8-wire modular connectors used for 10BASE-T networks. It is similar to, but wider than, the standard (RJ-11) telephone modular connectors.

RMON

Remote Monitoring Management Information Base (MIB). Uses SNMP and standard MIB design to provide multivendor interoperability between monitoring products and management stations.

RMS

Resource Management System. A set of protocols used by Datapoint to communicate from client stations to servers.

RNR

Receive Not Ready. An LLC and HDLC command or response indicating that transmission is blocked.

router

An internet linking device operating at the network layer (ISO layer 3).

RPC

Remote Procedure Call. A protocol for activating functions on a remote station and retrieving the result. Interpreted in the Sun PI suite. A similar protocol exists in Xerox XNS.

RPL	Remote Program Load. A protocol used by IBM on the IEEE 802.5 token ring network to download initial programs into networked stations. Interpreted in the IBM PI suite.
RPS	Ring Parameter Server. A station on a token ring network that maintains MAC-layer information about the LAN configuration such as ring numbers and physical location identifiers.
RR	Receive ready. An LLC non-data frame indicating readiness to receive data from the other station.
RS232 or RS-232C	Recommended Standard 232. EIA standard defining electrical characteristics of the signals in the cables that connect a DTE and a DCE.
RSTAT	Remote status. A protocol with the Sun NFS family used to exchange statistics on network activity. Interpreted in the Sun PI suite.
RTMP	Routing Maintenance Protocol. Used in AppleTalk networks to allow internet routers dynamically to discover routes to the various networks of an internet. A node that is not a router uses a subset of RTMP (the RTMP stub) to determine the number of the network to which it is connected and the node IDs of routers on its network. Interpreted in the AppleTalk protocol interpreter.
RTP	Routing Update Protocol. RTP is a protocol used to distribute network topology information. It was used prior to Version 5.5 of Banyan VINES.
RTS	Request To Send. A signal used in serial communications; sent, as from a computer to its modem, to request permission to transmit. RTS is a hardware signal sent over line 4 in RS-232C connections.
RU	Request Unit/Response Unit. The part of an SNA frame after the RH that contains the details of a request or its response.
RUnix	Remote Unix. A protocol atop TCP/IP for issuing remote requests over the network to a UNIX host.
S	Supervisory. An LLC, HDLC, or SDLC frame type used for control functions.

SABM
Set Asynchronous Balanced Mode. An LLC non-data frame requesting the establishment of a connection over which numbered Information frames may be sent.

SABME
Set Asynchronous Balanced Mode (Extended). SABM with two more bytes in the control field. Used in LAPB.

SAC
Single Attachment Concentrator. A concentrator that offers one S port for attachment to the FDDI network and M ports for the attachment of stations or other concentrators.

SAP
Service Access Point.

(1) A small number used by convention or established by a standards group, that defines the format of subsequent LLC data; a means of demultiplexing alternative protocols supported by LLC.

(2) Service Advertising Protocol. Used by NetWare servers to broadcast the names and locations of servers and to send a specific response to any station that queries it.

SARP
Sequenced Address Resolution Protocol. A protocol within Banyan VINES for finding a node's DLC address from its IP address. Interpreted in the Banyan VINES PI suite. *See also* **ARP**.

SAS
Single Attachment Station. An FDDI station that offers one S port for attachment to the FDDI ring.

SBI
Stop Bracket Initiation. An SNA message sent to request that the other station not initiate any more brackets.

SC
Session Control. An SNA subprocess for establishing and maintaining connections.

SCP
Session Control Protocol. The DECnet protocol concerned with the establishment of virtual circuits over which NSP transfers data; interpreted in the DECnet PI suite.

SDLC
Synchronous Data Link Control. An older serial communications protocol that was the model for LLC and with which it shares many features.

semaphore
A synchronization mechanism on an operating system.

serial interface

An interface which requires serial transmission, or the transfer of information in which the bits composing a character are sent sequentially. Implies only a single transmission channel.

Session

Name for the session-layer protocol in the ISO series, interpreted in the ISO PI suite.

SIA

Sniffer Internetwork Analyzer. Network General's internetwork analyzer that provides diagnostic capabilities by encapsulating LAN protocols running over leased line, Frame Relay, or X.25 circuits.

SIF

Status Information Frame. Used by stations on an FDDI ring to exchange information about station configuration and operating parameters.

SIG

Signal. A high-priority SNA message used to request permission to send.

SMB

Server Message Block. A message type used by the IBM PC LAN Program to make requests from a user station to a server and receive replies. Many of the functions are similar to those made by an application program to DOS or to OS/2 running on a single computer.

SMT

Station Management. Provides ring management, connection management, and frame services for an FDDI ring.

SMTP

Simple Mail Transfer Protocol. A protocol within TCP/IP for reliable exchange of electronic mail messages. Interpreted in the TCP/IP PI suite.

SNA

(1) Systems Network Architecture. A set of protocols used by IBM for network communications, particularly with mainframe computers. Interpreted in the IBM PI suite.

(2) Sniffer Network Analyzer. Network General's network analyzer that attaches to a network to monitor, record, analyze, and interpret network transmissions. Monitoring and analysis functions are separate menu-driven activities that provide high-level analysis and troubleshooting for complex local and wide area network installations.

SNAP

Subnetwork Access Protocol (sometimes called Subnetwork Access Convergence Protocol). An extension to IEEE 802.2 LLC that permits a station to have multiple network-layer protocols. The protocol specifies that DSAP and SSAP addresses must be AA hex. A field subsequent to SSAP identifies one specific protocol. Interpreted in the TCP/IP PI suite and the AppleTalk PI suite.

SNDCP

Subnetwork Dependent Convergence Protocol. SNDCP is an intermediate protocol that provides an interface between X.25 and the transport layer of an ISO protocol. (The enclosed ISO protocols are interpreted when the ISO PI suite is also installed.)

Sniffer Server

The Distributed Sniffer System (DSS) server that captures and analyzes packet-level network data under instructions from the client, a DSS SniffMaster Console. The Server is a computer that uses proprietary software and hardware. The Sniffer Server has both an analysis and an advanced monitoring application which are based on similar applications found on the Sniffer Network Analyzer. The Server uses two network interface cards: a Transport Card that supports communication with Consoles and a Monitor card that is used to capture frames and collect statistics from the network.

SniffMaster Console

The Distributed Sniffer System (DSS) *client* that communicates with the DSS Sniffer Servers from any point on the network. The Console delivers instructions to the Server and reads the output of the Server's analysis. The Console is a computer that uses proprietary software and hardware. The proprietary hardware is a network interface card called a Transport Card for communicating over the network with Servers.

SNMP

Simple Network Management Protocol. Interpreted in the TCP/IP PI suite.

SNRM

Set Normal Response Mode. Places a secondary station in a mode that precludes it from sending unsolicited frames. The primary station controls all message flow. Used in SDLC.

SNRME

Set Normal Response Mode (Extended). SNRM with two more bytes in the control field. Used in SDLC.

socket A logically addressable entity or service within a node, serving as a more precise identification of sender or recipient.

SoftTalk SoftTalk. SoftTalk is a session-level protocol that includes support for remote procedure calls used to support TOPS.

source address The part of a message that indicates from whom the message came.

spanning tree A method of creating a loop-free logical topology on an extended LAN. Formation of a spanning tree topology for transmission of messages across bridges is based on the industry-standard spanning tree algorithm defined in IEEE 802.1d.

SPP Sequenced Packet Protocol.

(2) The transport-layer protocol that provides virtual connection service in Banyan VINES, based upon the protocol of the same name in XNS. Interpreted in the Banyan VINES PI suite.

SPX Sequential Packet Exchange. Novell's version of the Xerox protocol called SPP. Interpreted in the Novell NetWare PI suite.

SQE Signal Quality Error. The 802.3/Ethernet collision signal from the transceiver.

SQE TEST The SQE signal generated by the transceiver at the end of a transmitted frame to check the SQE circuitry. Also known as *heartbeat* in Ethernet.

SRF Status Report Frames (SRFs) are used to periodically announce station status that may be of interest to the manager of an FDDI ring.

SRTP Sequenced Routing Update Protocol. Used to distribute network topology information (Banyan VINES Version 5.5 and later). Interpreted in the Banyan VINES PI suite. *See also* **RTP**.

SS7 Signaling System 7. Protocol related to ISDN. Directs how the interior of an ISDN network is managed.

SSAP
Source Service Access Point. The LLC SAP for the protocol used by the originating station.

SSCP
System Services Control Point. An SNA identification of communications management functions.

StreetTalk
Protocol used in Banyan VINES to maintain a distributed directory of the names of network resources. In VINES names are global across the internet and independent of the network topology. Interpreted in the Banyan VINES PI suite.

SUA
Stored Upstream Address. The network address of a token ring station's nearest upstream neighbor. Texas Instruments calls this the UNA.

subnet
A term used to denote any networking technology that makes all nodes connected to it appear to be one hop away. In other words, the user of the subnet can communicate directly to all other nodes on the subnet. A collection of subnets together with a routing or network layer combine to form a network.

SVC
Switched Virtual Circuit. A virtual circuit that is set up on demand, as in the case of a dial-up telephone line, or an X.25 call.

symptom
An abnormal or unusual network event which the Expert Sniffer analyzer detects. A symptom is indicative of a possible network problem.

synchronous transmission
A method of data transfer in which information is transmitted in blocks (frames) of bits separated by equal time intervals.

T1
A digital transmission link with a capacity of 1.544 Mbps.

TC
Transmission Control. An SNA subprocess.

TCP
Transmission Control Protocol. The connection-oriented byte-stream protocol within TCP/IP that provides reliable end-to-end communication by using sequenced data sent by IP. Interpreted in the TCP/IP PI suite.

TCP/IP
Transmission Control Protocol/Internet Program. A suite of networking protocols developed originally by the US Government for ARPANET and now used by several LAN manufacturers. The individual TCP/IP protocols are listed separately in this Glossary.

TDS
Sybase's Tabular Data Stream. An application-level protocol used to send requests and responses between clients and servers.

TELNET
Protocol for transmitting character-oriented terminal (keyboard and screen) data. Interpreted in the TCP/IP PI suite.

terminator
A resistive connector used to terminate the end of a cable or an unused tap into its characteristic impedance. The terminator prevents interference-causing signal reflections from the ends of the cable.

TFTP
Trivial File Transfer Protocol. A protocol within TCP/IP used to exchange files between networked stations. Interpreted in the TCP/IP PI suite.

TH
Transmission Header. The initial part of an SNA frame immediately following the LLC header.

THT
Token Holding Timer. The maximum length of time a station holding the token can initiate asynchronous transmissions. The THT is initialized with the value corresponding to the difference between the arrival of the token and the TTRT (FDDI).

TNS
Transparent Network Substrate. Provides database applications with a single common interface to all industry-standard network protocols.

token
A small message used in some networks to represent the permission to transmit; it is passed from station to station in a predefined sequence.

token bus
A type of LAN where all stations can hear what any station transmits and where permission to transmit is represented by a token sent from station to station.

token ring
A ring-shaped LAN where each station can directly hear transmissions only from its immediate neighbor. Permission to transmit is granted by a token that circulates around the ring.

TOPS
A presentation-layer protocol used for remote access to files across different operating systems. Interpreted in the AppleTalk protocol interpreter suite.

TP
Transport-layer Protocol. It exists in alternate forms, depending on how the services it assumes are provided to it by the network layer below it. TP 0 assumes that the connection is maintained at the lower layer, while TP 4 assumes a connectionless network protocol, so that functionality for the establishment and maintenance of a connection are included in the transport protocol. Layers 0, 2, and 4 are interpreted in the ISO PI suite.

Transport
Layer 4 of the OSI reference model. The transport layer is responsible for reliable network communication between end nodes. It implements flow and error control and often uses virtual circuits to ensure reliable data delivery.

trigger
A Sniffer analyzer feature that allows a user to define an event after which the analyzer will stop capture to ensure that frames preceding and/or following the event are retained in the capture buffer.

TRLR
Trailer format. Variant of IP in which the protocol headers follow rather than precede the user data.

TRT
Token Rotation Timer. A clock that times the period between the receipt of tokens (FDDI).

TS
Transmission Services. An SNA subprocess.

TSR
Terminate and Stay Resident. A DOS program that once loaded into RAM, remains there in the background until unloaded or power is shut off.

TTRT
Target Token Rotation Timer. The value used by the MAC receiver to time the operations of the MAC layer. The TTRT value varies depending on whether or not the ring is operational (FDDI).

TVX Valid Transmission Timer. A timer that times the period between valid transmissions on the ring; used to detect excessive ring noise, token loss, and other faults (FDDI).

UA Unnumbered Acknowledgment. An LLC frame that acknowledges a previous SABME or DISC request.

UDP User Datagram Protocol. A protocol within TCP/IP for sending unsequenced data frames not otherwise interpreted by TCP/IP.

UI Unnumbered Information. An LLC, HDLC, or SDLC frame type used to send data without sequence numbers.

UNA Upstream Neighbor Address. The network address of a token ring station's nearest upstream neighbor. IBM calls this the SUA.

UNIX A popular portable operating system written by AT&T.

V.35 A CCITT wideband interface recommendation for WANs.

VINES VIrtual NEtwork Software. The networking operating system developed by Banyan Systems Inc., and the protocols used therein. Notable components are StreetTalk and Net RPC.

VIP VINES Internet Protocol. The lowest-layer protocol in Banyan VINES that is responsible for end-to-end forwarding and long packet fragmentation control. Interpreted in the Banyan VINES PI suite. A similar protocol is interpreted in the TCP/IP PI. *See also* **VINES**, **IP** and **ISO IP**.

virtual circuit A communications link that appears to be a dedicated point-to-point circuit.

VMTP Versatile Message Transaction Protocol (proposed).

VT Virtual Terminal. An entity that is part of the application-layer protocol and permits an application to interact with a terminal in a consistent manner independent of the terminal characteristics.

VTP Virtual Terminal Protocol. The protocol used for an application to interact with a virtual terminal.

WAN	Wide Area Network. A collection of LANs, or stations and hosts, extending over a wide area that can be connected via common carrier or private lines. Typically, transmission speeds are lower on a WAN than on a LAN.
X.25	A CCITT recommendation that defines the standard communications interface for access to packet-switched networks.
X.400	ISO standard protocol for electronic mail. Interpreted in the ISO PI suite.
X.500	ISO standard protocol for directory services. Similar to DNS and NIS.
XID	Exchange Identification. An LLC unnumbered frame type used to negotiate what LLC services will be used during a connection.
X.nn	CCITT Recommendation designation, such as X.25 protocol.
XNS	Xerox Network Systems. A family of protocols standardized by Xerox, in particular the Internet Transport Protocols.
X Window	Protocol for the management of high-resolution color windows at workstations, originated by MIT, DEC, and IBM and subsequently transferred to a consortium of vendors and developers.
YP	Yellow Pages. A protocol developed by Sun Microsystems for implementing a distributed resource look-up database; similar in function to DNS. Interpreted in the Sun PI suite. Now called NIS.
ZIP	Zone Information Protocol. Used in AppleTalk to maintain an internet-wide mapping of networks to zone names. ZIP is used by the Name-Binding Protocol (NBP) to determine which networks belong to a given zone. Interpreted in the AppleTalk PI suite.
Zone	In AppleTalk networks, a set of one or more nodes within an internet.

Appendix B
Bibliography

General References

Martin, James. *Local Area Networks*. The Arben Group, 1989.

Meijer, Anton and Paul Peeters. *Computer Network Architectures*. Rockville, Maryland: Computer Science Press, 1982.

Stallings, William. *Local Networks*. Macmillan, 1990.

Tannenbaum, Andrew S. *Computer Networks*. 2d ed. Englewood Cliffs, New Jersey: Prentice Hall, 1989.

Network References

Ethernet

IEEE Standards for Local Area Networks: *Logical Link Control*. ANSI/IEEE Std 802.2-1985 (ISO/DIS 8802/2). IEEE publication number SH09712. Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017.

IEEE Standards for Local Area Networks: *Carrier Sense Multiple Access with Collision Detection (CSMA/CD). Access Method and Physical Layer Specifications.* ANSI/IEEE Std 802.3-1985 (ISO/DIS 8802/3). IEEE publication number SH09738. Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017.

The Ethernet: A Local Area Network. Data Link Layer and Physical Layer Specifications. ("The blue book.") Issued jointly by Digital Equipment Corporation, Maynard, MA, Intel Corporation, Santa Clara, CA, and Xerox Corporation, Stamford, CT. Version 2.0, November 1982. Available from: Hillary Cornell, Xerox Systems Institute, 475 Oakmead Parkway, Sunnyvale, CA 94086. (408) 737-4652.

Token Ring

Haugdahl, J. Scott. *Inside the Token Ring*. Architecture Technology Corporation, 1986. P.O. Box 24344, Minneapolis MN 55424.

IEEE Standards for Local Area Networks: Logical Link Control. ANSI/IEEE Std 802.2-1985 (ISO/DIS 8802/2). IEEE publication number SH09712. Institute of Electrical and Electronics Engineers, 345 East 47th Street, New York, NY 10017.

IEEE Standards for Local Area Networks: Token Ring Access Method. ANSI/IEEE Std 802.5-1985 (ISO/DP 8802/5), IEEE publication number SH09944.

TMS380 Adapter Chipset User's Guide. Texas Instruments Incorporated, publication number SPWU001.

Token Ring Network Architecture Reference. IBM Corporation, publication number 6165877.

Token Ring Network PC Adapter Technical Reference. IBM Corporation, publication number 69X7713.

FDDI

American National Standard for Information Systems. *Fiber Distributed Data Interface (FDDI) - Token Ring Media Access Control (MAC).* ANSI X3.139-1987. American National Standards Institute, 1987.

American National Standards for Information Systems. *Fibre Data Distributed Data Interface (FDDI) - Token Ring Physical Layer Medium Dependent (PMD).* ANSI X3.166-1990. American National Standards Institute, 1990.

A Primer to FDDI: Fiber Distributed Data Interface. Digital Equipment Corporation, 1991.

LocalTalk

Sidhu, Gursharan S., Richard F. Andrews and Alan B. Oppenheimer. *Inside AppleTalk.* Addison-Wesley Publishing Company, 1989.

Synchronous

Data Communication Networks Interfaces: Recommendations X.20—X.32, Red Book, Volume VIII-Fascicle VIII.3. Geneva: International Telecommunications Union-CCITT, 1985.

ATM

McDysan, David E. and Spohn, Darren L. *ATM Theory and Application*. McGraw-Hill, Inc., 1995.

User-Network Interface (UNI) Specification, Version 3.1. The ATM Forum Technical Committee. September, 1994.

Protocol References

IBM

Advanced Program-to-Program Communication for the IBM Personal Computer. Programming Guide. IBM Corporation, publication number 61X3842.

Haugdahl, J. Scott. *Inside NetBIOS*. Architecture Technology Corporation, 1986. P.O. Box 24344, Minneapolis MN 55424.

Systems Network Architecture Reference Summary. IBM Corporation, publication number GA27-3136.

Novell NetWare

Sheldon, Tom. *Novell NetWare: The Complete Reference*. Berkeley, California: McGraw-Hill, 1989.

XNS

Internet Transport Protocols. Xerox Systems Integration Standard X.S.I.S. 028112, December 1981.

TCP/IP

Cerf, V.G. and R.E. Kahn. "A Protocol for Packet Network Interconnection." *IEEE Trans. Commun*. COM-22:637—648 (May 1974).

Comer, Douglas E. *Internetworking With TCP/IP: Principles, Protocols, and Architecture*. Englewood Cliffs, New Jersey: Prentice-Hall, 1988.

DDN Protocol Handbook.
Vol. 1: DOD Military Standard Protocols. NIC-5004.
Vol. 2: DARPA Internet Protocols. NIC-5005.
Vol. 3: Supplement. NIC-5006.
US Defense Communications Agency, December 1985. Available from: DDN Network Information Center, DDN Network Information Center, SRI

International, Room EJ291, 333 Ravenswood Avenue, Menlo Park, CA 94025 (800) 235-3155; (415) 859-3695. NIC@SRI-NIC.ARPA;
or from Defense Technical Information Center, Cameron Station, Alexandria, VA 22314 (202) 274-7633.

OSI

Day, J.D. and H. Zimmerman. "The OSI Reference Model." *Proceedings of the IEEE* 71 (1983): 1334-1340.

Henshall, J. and A. Shaw. *OSI Explained. End to End Computer Communication Standards.* Chichester, England: Ellis Horwood, 1988.

Linington, P.F. "Fundamentals of the Layer Service Definitions and Protocol Specifications." *Proceedings of the IEEE* 71 (1983): 1341-1345.

Rose, Marshall T. *The Open Book: A Practical Perspective on OSI.* Englewood Cliffs, New Jersey, 1990.

Zimmerman, H. "OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection." *IEEE Trans. Commun.* COM-28:425—432 (April 1980).

DECnet

Malamud, Carl. *DEC Networks and Architectures.* New York: McGraw-Hill Book Company, 1989.

AppleTalk

Sidhu, Gursharan S., Richard F. Andrews and Alan B. Oppenheimer. *Inside AppleTalk.* Addison-Wesley Publishing Company, 1989.

X Window

Scheifler, Robert, James Gettys, and Ron Newman. *X Window System, Library, and Protocol Reference.* Digital Press, 1988.

X.25

Deasington, R.J. *X.25 Explained: Protocols for Packet Switched Networks.* 2d ed. Chichester, England: Ellis Horwood, 1988.

Dhas, C.R. and V.K. Konangi. "X.25: An Interface to Public Packet Networks." *IEEE Commun. Magazine* IT-22 (1976): 118-125.

The X.25 Protocol and Seven Other Key Protocols. Belmont, California: Lifetime Learning Publications.

SNA

IBM Systems Network Architecture Formats. IBM Corporation, publication number GA27-3136-10

SMT

A Primer to FDDI: Fiber Distributed Data Interface. Digital Equipment Corporation, 1991.

ATM

McDysan, David E. and Spohn, Darren L. *ATM Theory and Application.* McGraw-Hill, Inc., 1995.

User-Network Interface (UNI) Specification, Version 3.1. The ATM Forum Technical Committee. September, 1994.

LAN Emulation Over ATM, Version 1.0. The ATM Forum Technical Committee. January, 1995.

Index

D

E

F

G

H

I

J

K

L

M

Q

R

S

T

U

Network General

TOTAL NETWORK VISIBILITY™

Corporate Headquarters
Network General Corporation
4200 Bohannon Drive
Menlo Park, CA 94025 USA
Tel: (415) 473-2000

Network General UK Ltd.,
Royal Albert House, Sheet Street
Windsor, Berkshire, SL4 1BE, England
Tel: (44) 1753-863400
Fax: (44) 1753-863407

Network General Canada, Ltd.
100 Mural Street, Suite #203
Richmond Hill, Ontario L4B 3J6 Canada
Tel: 1 (905) 709-9155
Fax:1 (905) 709-9180

P/N: 3005303